SWAF

Semantic based Web Application Firewall (SWAF V 1.6)

Operations and User Manual

Document Version – 1.0

Table of Contents

1 SWAF 4

1.1 SWAF Features 4

2 Operations and User Manual 7

2.1 SWAF Administrator Panel: 8

2.1.1 System Monitor Menu: 9

2.1.2 Traffic Analyzer: 15

2.1.3 Statistics Menu: 21

2.1.4 Configurations 28

2.1.5 User Management 41

2.1.6 Audit Log Menu 43

3 Case Study 46

3.1 Example scenario # 1 47

3.2 Configuring a Web Application with SWAF 47

3.3 Example scenario # 2 48

3.3.1 Creating a new user 48

3.3.2 Assigning role to a User 50

3.3.3 Creating a User Role 51

Glossary 54

List of Figures

Figure 1: login screen 8
Figure 2: CPU Load 10
Figure 3: Access Traffic Load 11
Figure 4: Infected Traffic Load 11
Figure 5: Traffic Comparison 12
Figure 6: Application Monitor 13
Figure 7: System State Screen 14
Figure 8: System Info 14
Figure 9: Top Traffic Originators 15
Figure 10: Top Traffic Originators Ratio 16
Figure 11: Current Traffic 16
Figure 12: Top Infected Traffic Originators 17
Figure 13: Top Infected Traffic Originators Ratio 18
Figure 14: Current Infected Traffic Detail 18
Figure 15: Access Log Search 19
Figure 16: Current Infected Traffic Details 21
Figure 17: Access Traffic 22
Figure 18: Access Traffic Ratio 23
Figure 19: Access Traffic Details 24
Figure 20: Infected Traffic 25
Figure 21: Infected Traffic Ratio 25
Figure 22: Infected Traffic Detail 26
Figure 23: Attacks Ratio 27
Figure 24: CPU Utilization 27
Figure 25: Configuration 28
Figure 26: Log Configurations 29
Figure 27: Proxy Configurations 31
Figure 28: Email Configuration 32
Figure 29: Protocol Validation Configurations 34
Figure 30: DoS Configurations 36
Figure 31: Stateful Attacks Configuration 37
Figure 32: Web Application Configurations 38
Figure 33: DB Backup 39

Figure 34: Configuration Backup 40
Figure 35: Update Rules Files 41
Figure 36: User Management 41
Figure 37: User Management 42
Figure 38: Group Rights 43
Figure 39: Audit Log 44
Figure 42: Web Application Configuration 47
Figure 43: Add Web Application 48
Figure 44: Successful creation of Web Application 48
Figure 45: User Management 49
Figure 46: Create User 49
Figure 47: New User Creation 50
Figure 48: Successful Creation of User 50
Figure 49: Role Rights 51
Figure 50: Creating New Role 51
Figure 51: Create Role 52

1 SWAF

SWAF is a Web Application Firewall which is capable of protecting web applications against all types of application layer attacks, known or unknown. It is built using a hybrid security model that permits only valid application behavior to be executed, without relying on attack signatures. It analyzes bidirectional traffic including SSL-encrypted communication and uses Semantics based techniques to verify and validate the traffic, which enables SWAF to provide protection against OWASP Top Ten attacks and many more application level vulnerabilities, without making any changes to the target application.

1.1 SWAF Features

SWAF provides real-time web application security. SWAF is capable of protecting against Zero day attacks, which is still an unattainable goal for existing WAF solutions. In addition to this SWAF possess the following distinguishing features:

1. **Semantics based Analysis and Rule Generation:**

   SWAF uses semantic based techniques to understand the context of user input which helps detect abnormal behavior and facilitates in providing a sturdy defense mechanism against OWASP top ten attacks and other complex attacks. Automatic rule generation improves attack detection mechanism. Analysis is carried out using the reasoning ability provided by semantics.

2. **Automated Application Profiling:**

   SWAF supports automated application profiling. The profile is semantically saved and the positive security model is developed by utilizing the reasoning ability provided by ontologies.

3. **Inbound and Outbound traffic analysis and filtering:**

It analyzes all the bi-directional traffic and scrutinizes it for abnormal behavior.

4. **SSL Attacks Detection:**

   SWAF also has the capability to protect SSL encrypted traffic. It intercepts the bi-directional SSL traffic stream and decrypts traffic to scrutinize it for malicious behavior.

5. **HTTP Protocol Validation:**

   SWAF not only provide content filtering but also perform HTTP protocol enforcement. If the packet presents HTTP protocol violation, it is considered invalid and hence discarded.

6. **Comprehensive Security using Hybrid Security Model:**

   SWAF is built using a hybrid security model which provides an optimized solution where both positive and negative security models complement each other to provide comprehensive level of security.

7. **PCI compliance**

   SWAF is built to be PCI DSS (Payment Card Industry Data Security Standard) compliant.

8. **Better Performance:** SWAF is designed to deliver performance as it provides deep packet inspection and content filtering on the basis of semantic information related to protocol, application and attacks, resulting in effective, efficient and reliable security system. Following features are built to enhance performance of the system:

   - **SSL Offloading**

     SSL offloading relieves the Web server of the processing burden of encrypting and/or decrypting traffic sent via SSL.

- **Load balancing**

  Load balancing distributes traffic efficiently among network servers so that no individual server gets overburdened

- **Http traffic compression Caching**

  Caching helps improve the following two factors to enhance the speed of Web applications:

  ✓ Reducing the number of request/response roundtrips.
  ✓ Reducing the number of bytes transferred between the server and the client.

Similarly HTTP Compression can dramatically decrease the number of bytes that are transmitted between the server and the client. SWAF supports HTTP caching and compression to improve on the performance of the application.

9. IP filtering:

SWAF has IP filtering capability.

10. Rate Control:

SWAF optimizes rate of access to Web applications from different networks to mitigate DoS attack.

11. Easy Management:

Provide ease of management by producing integrated reports

12. Availability:

The system is built to be highly available. SWAF is designed to be available 24 hours throughout the week.

13. No Change in Target Application:

SWAF works as a security envelope for the web application and does not require any modifications to the target application.

2 Operations and User Manual:

The Operations and User Manual is designed to facilitate the user in understanding SWAF as a system. The document is divided into two sections the SWAF Administrator Panel and the case study. The first section gives a thorough guideline to understand the purpose of the menu and screens and all the field that reside inside a screen. The second section presents the SWAF usage scenario, providing stepwise description of how to manage users and configure web applications in SWAF.

Login Screen: To run SWAF it needs first to click the Register button and browse the license key. Then one can be able to login in.

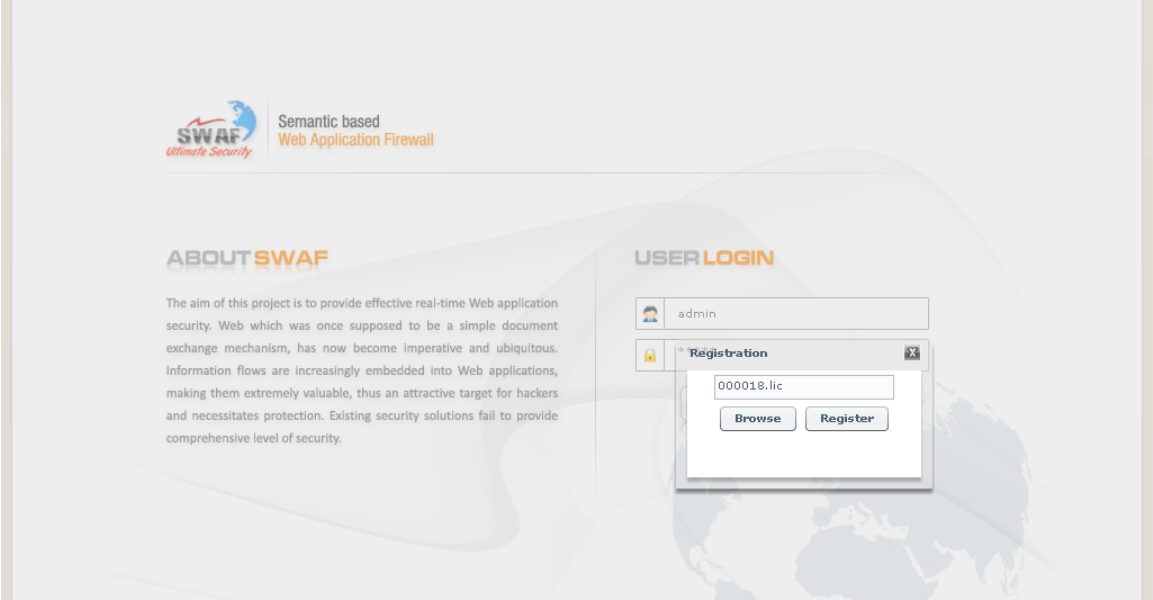
Semantic based
Web Application Firewall
ABOUT SWAF
The aim of this project is to provide effective real-time Web application security. Web which was once supposed to be a simple document exchange mechanism, has now become imperative and ubiquitous. Information flows are increasingly embedded into Web applications, making them extremely valuable, thus an attractive target for hackers and necessitates protection. Existing security solutions fail to provide comprehensive level of security.
USER LOGIN
admin
Registration
000018.lic
Browse
Register

Figure 1: login screen

.

2.1.1 SWAF Administrator Panel:

The administrator panel of SWAF enables the administrator to perform System Monitoring, Traffic Analysis, view statistics, set configurations, perform user management and view audit logs. The administrator can perform the above mentioned tasks by selecting the desired item from the menu displayed at left side of the screen. Figure 1. Presents the screenshot of the administrative panel.

Figure 2: Administrative Panel

Following section presents the details of the menu items and the screens associated with them.

2.1.2 System Monitor Menu:

2.1.2.1 CPU load:

Figure 2 shows the CPU utilization of SWAF machine and this graph is updated after every 5seconds.

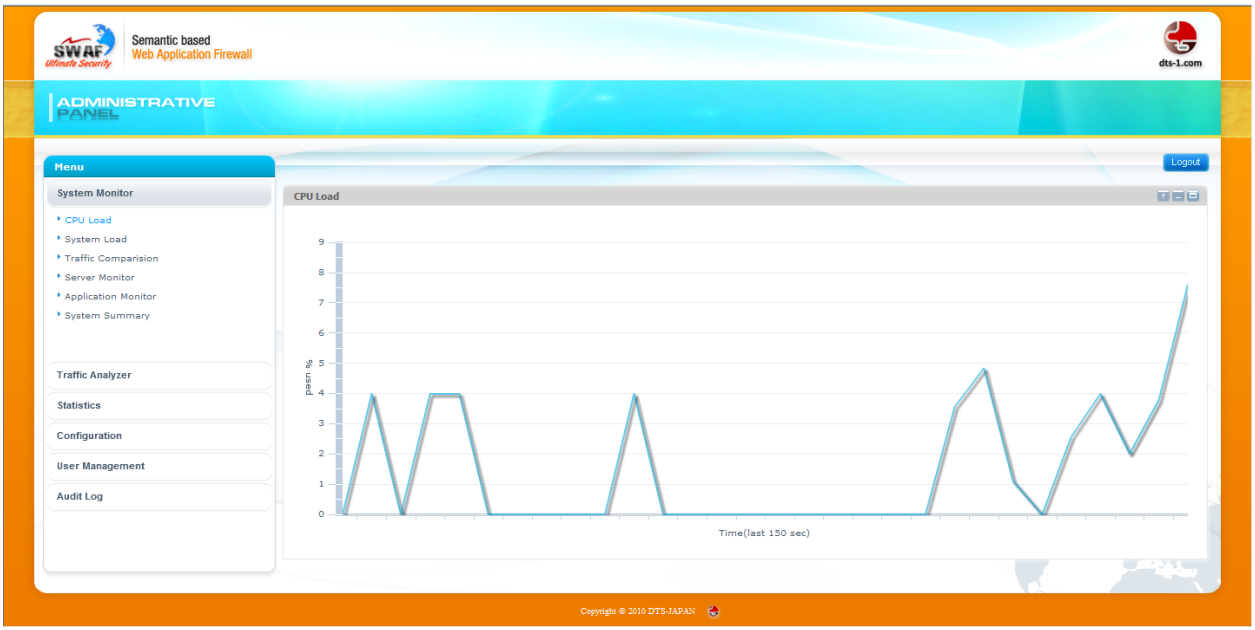

Figure 3: CPU Load

2.1.2.2 System Load:

This menu facilitates the user to system load in terms of access and infected traffic.

2.1.2.2.1 Access Traffic load Screen:

Figure 3 shows the system load of Access Traffic and number of hits generated by different IP addresses.

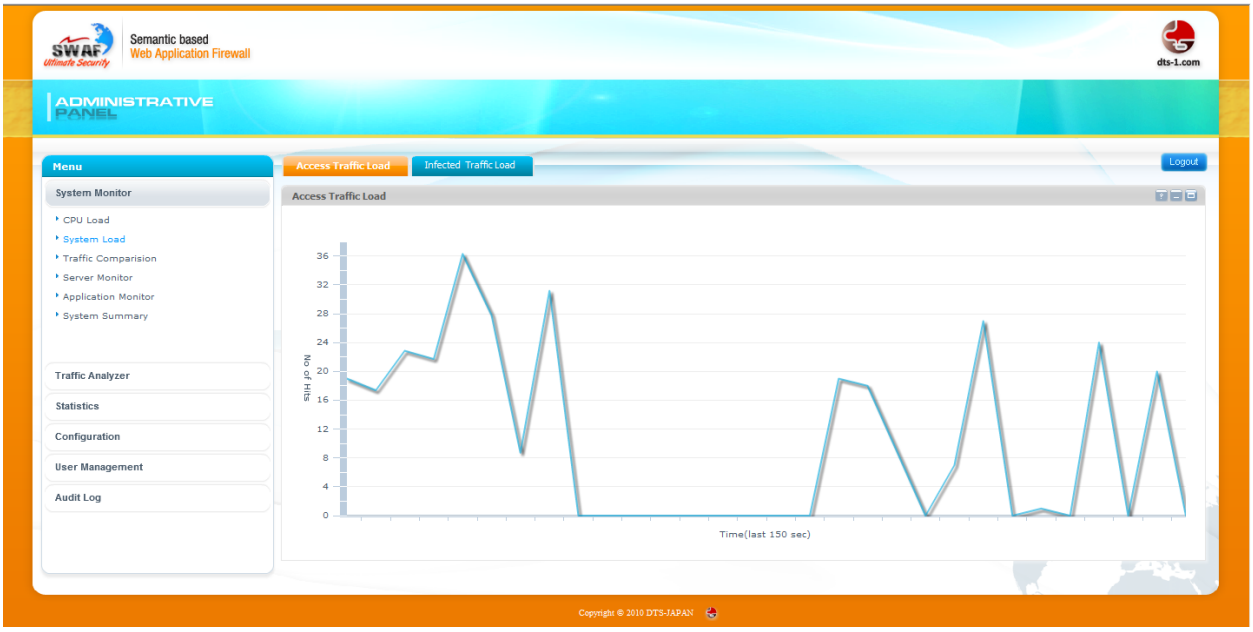

Figure 4: Access Traffic Load

2.1.2.2.2 Infected Traffic Load Screen:

This figure shows the system load of Infected Traffic.

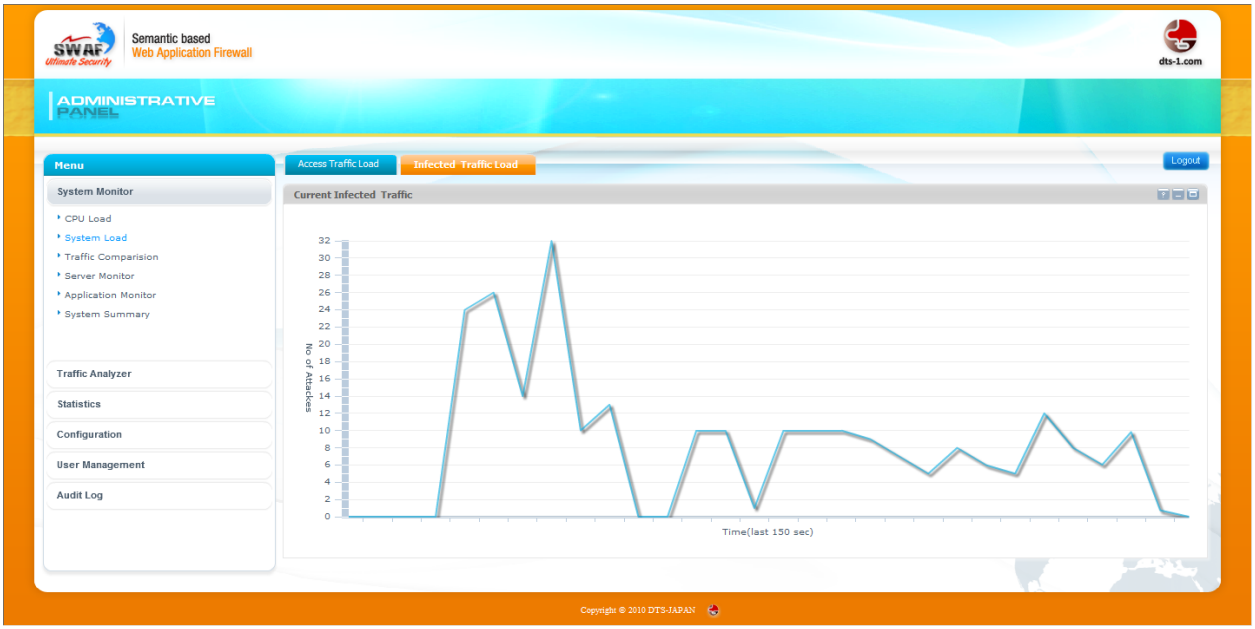

Figure 2: Infected Traffic Load

2.1.2.3 Traffic Comparison:

Figure 5 shows the comparison between access and infected traffic

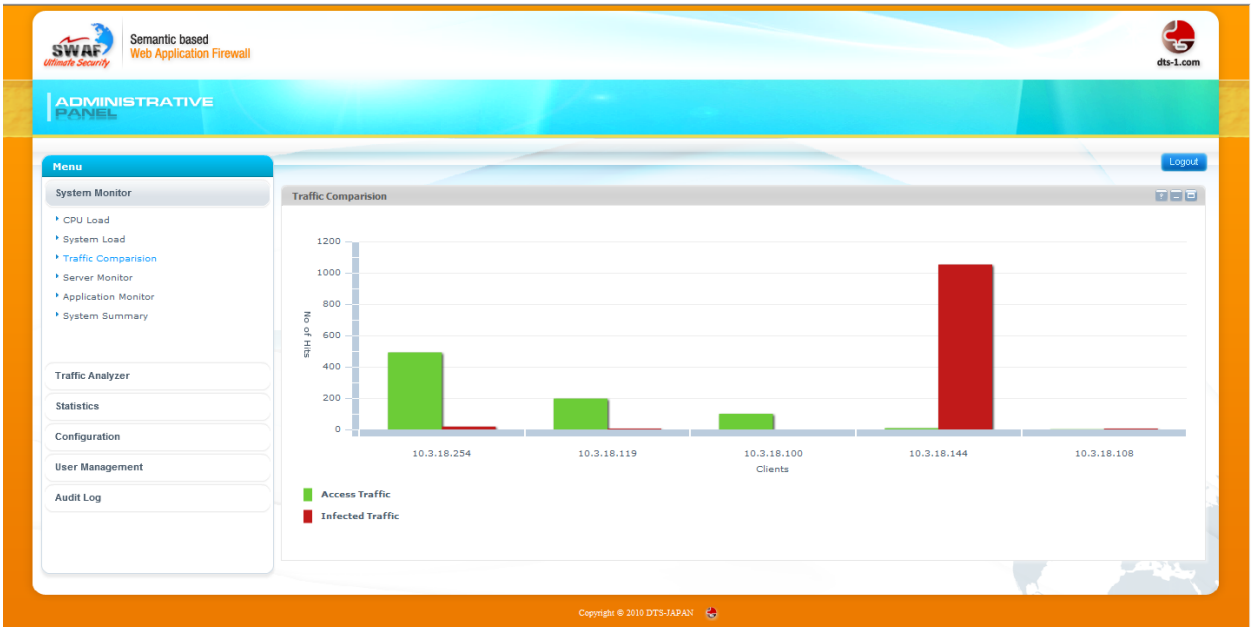

Figure 3: Traffic Comparison

2.1.2.4 Application Monitor Screen:

Figure shows the application monitor.

Application Name: IP address of application

Host IP address: IP address of Host

Traffic Count: count of generated traffic from different IPs

Infected Traffic Count: count of infected traffic generated from users.

2.1.2.5 Application Monitor Screen:

Figure 4: Application Monitor

2.1.2.6 System Summary Menu:

The system summary menu facilitates the administrator to monitor system state and view system information.

2.1.2.6.1 System State screen:

This figure shows the current state of system.

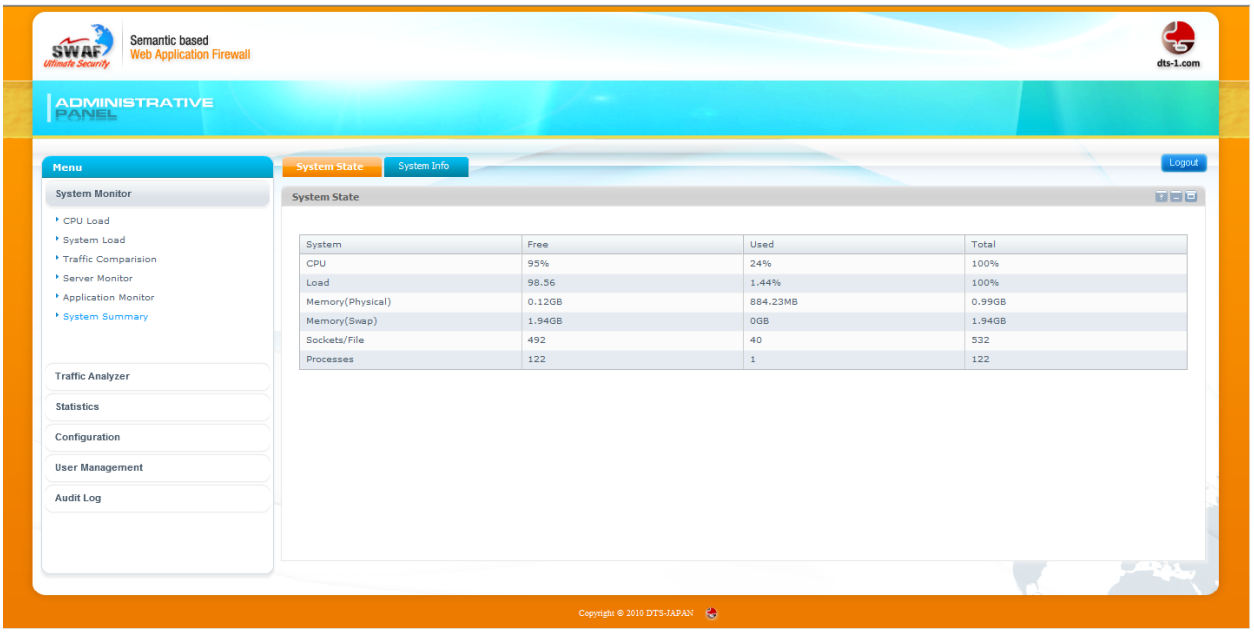

Figure 5: System State Screen

2.1.2.6.2 System Info Screen:

This figure shows the information about system

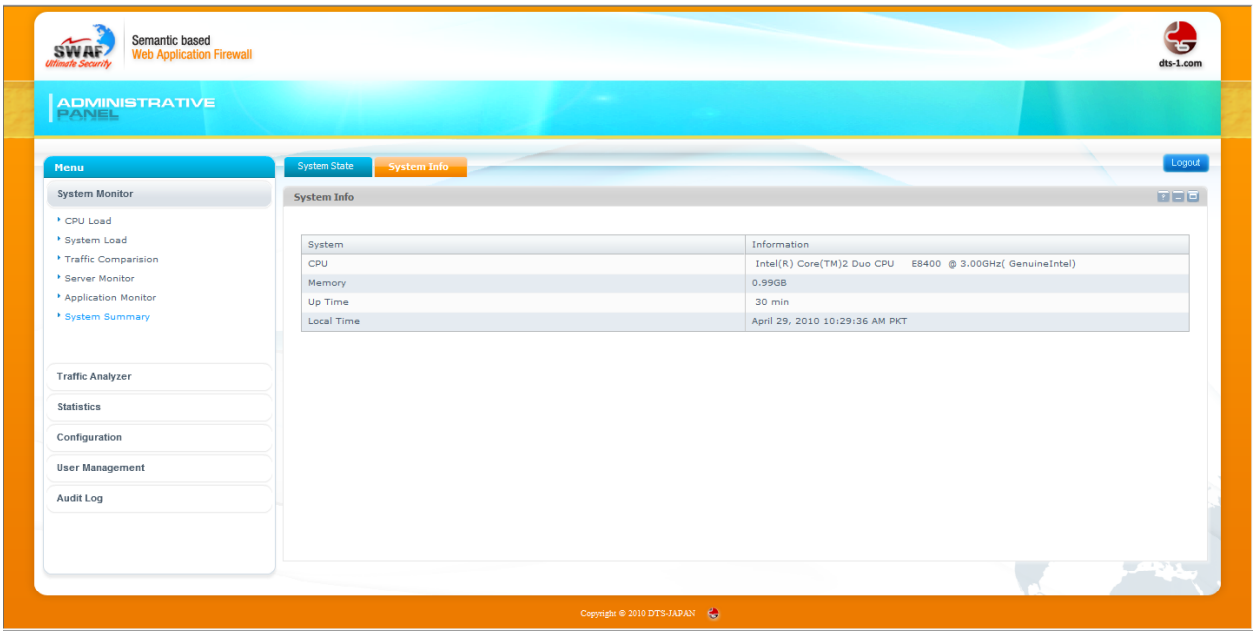

Figure 6: System Info

2.1.3 Traffic Analyzer:

Traffic analyzer menu provide the administrator the option to view access and infected traffic and search for the desired information.

2.1.3.1 Access Traffic Menu

Access traffic menu gives the administrator the option to view statistics related to access log. This information includes details of top traffic originators and their ratio and the current traffic passing through SWAF.

2.1.3.1.1 Top Traffic Originators Screen

This figure shows the traffic which is originated from different IPs.

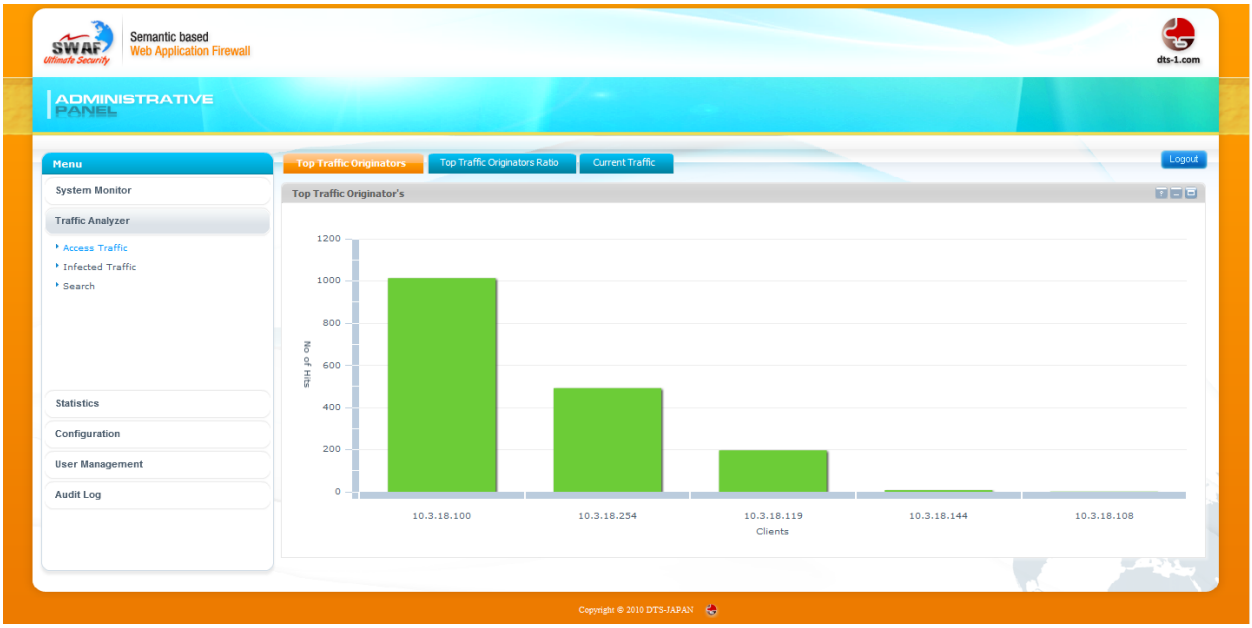

Figure 7: Top Traffic Originators

2.1.3.1.2 Top Traffic Originators Ratio Screen

This figure shows the ratio of Top Traffic Originators.

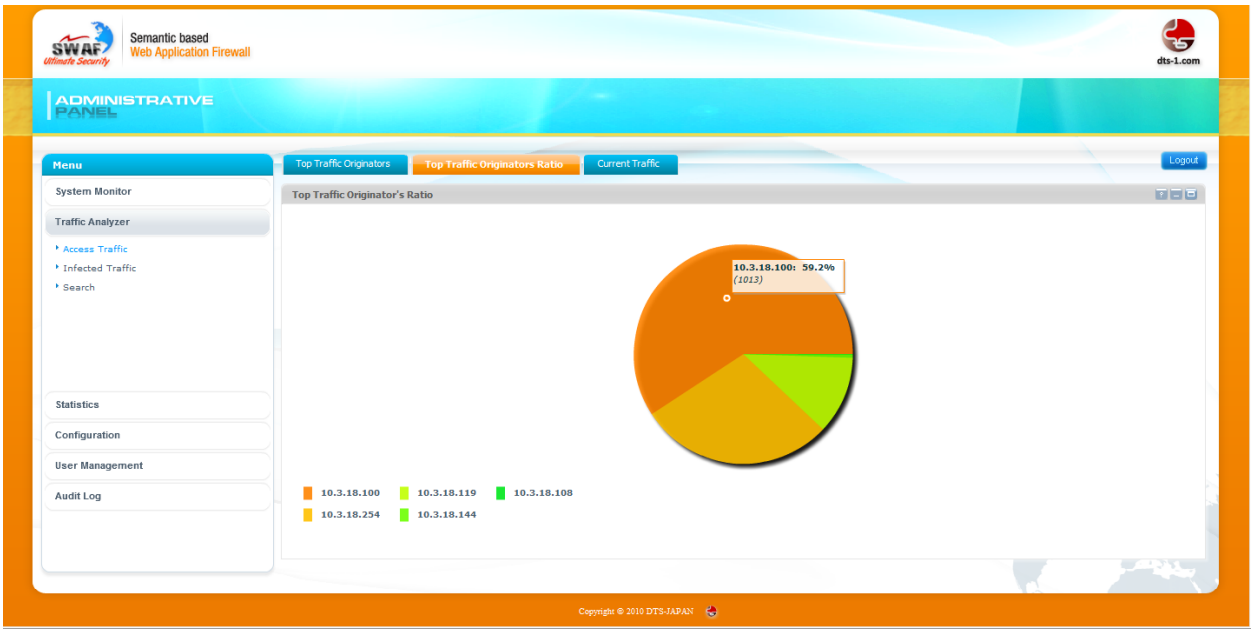

Figure 8: Top Traffic Originators Ratio

2.1.3.1.3 Current Traffic Screen

This screen shows the current traffic.

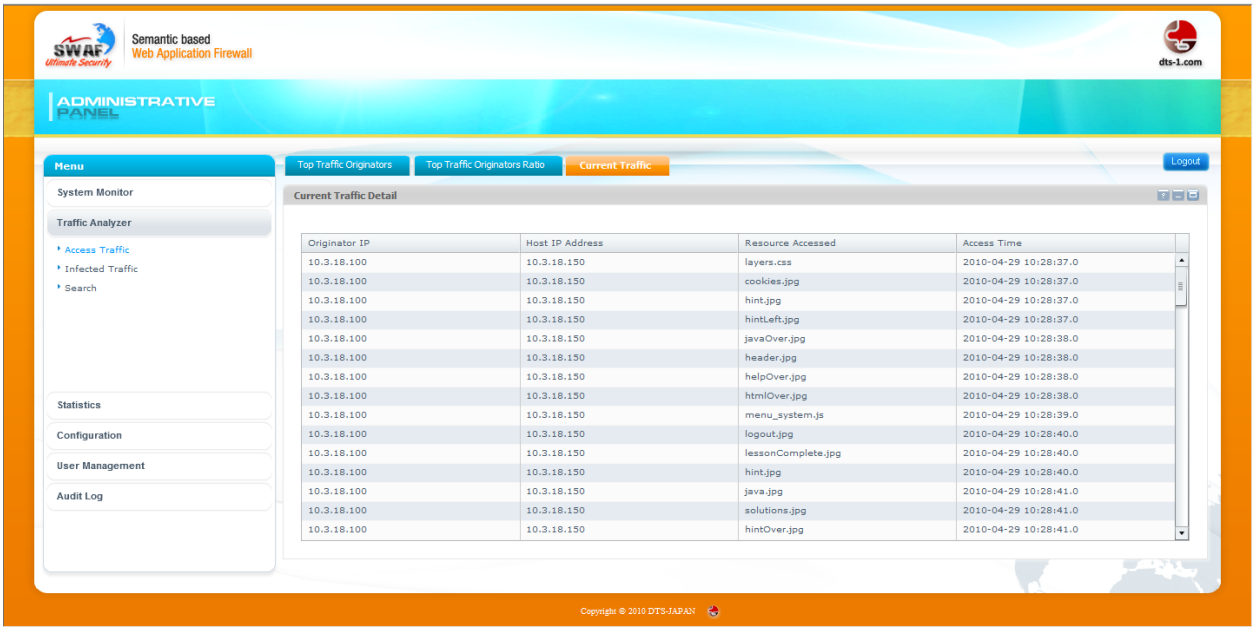
Semantic based
Web Application Firewall
dts-1.com
ADMINISTRATIVE
PANEL
Menu
System Monitor
Traffic Analyzer
Access Traffic
Infected Traffic
Search
Statistics
Configuration
User Management
Audit Log
Top Traffic Originators
Top Traffic Originators Ratio
Current Traffic
Logout
Current Traffic Detail
Originator IP | Host IP Address | Resource Accessed | Access Time
10.3.18.100 | 10.3.18.150 | layers.css | 2010-04-29 10:28:37.0
10.3.18.100 | 10.3.18.150 | cookies.jpg | 2010-04-29 10:28:37.0
10.3.18.100 | 10.3.18.150 | hint.jpg | 2010-04-29 10:28:37.0
10.3.18.100 | 10.3.18.150 | hintLeft.jpg | 2010-04-29 10:28:37.0
10.3.18.100 | 10.3.18.150 | javaOver.jpg | 2010-04-29 10:28:38.0
10.3.18.100 | 10.3.18.150 | header.jpg | 2010-04-29 10:28:38.0
10.3.18.100 | 10.3.18.150 | helpOver.jpg | 2010-04-29 10:28:38.0
10.3.18.100 | 10.3.18.150 | htmlOver.jpg | 2010-04-29 10:28:38.0
10.3.18.100 | 10.3.18.150 | menu_system.js | 2010-04-29 10:28:39.0
10.3.18.100 | 10.3.18.150 | logout.jpg | 2010-04-29 10:28:40.0
10.3.18.100 | 10.3.18.150 | lessonComplete.jpg | 2010-04-29 10:28:40.0
10.3.18.100 | 10.3.18.150 | hint.jpg | 2010-04-29 10:28:40.0
10.3.18.100 | 10.3.18.150 | java.jpg | 2010-04-29 10:28:41.0
10.3.18.100 | 10.3.18.150 | solutions.jpg | 2010-04-29 10:28:41.0
10.3.18.100 | 10.3.18.150 | hintOver.jpg | 2010-04-29 10:28:41.0
Copyright © 2010 DTS-JAPAN

Figure 9: Current Traffic

2.1.3.2 Infected Traffic Menu

Infected traffic menu gives the administrator the option to view statistics related to infected log. This information includes details of top infected traffic originators and their ratio and the current infected traffic details.

2.1.3.2.1 Top Infected Traffic Originators Screen

This figure shows the infected traffic which is originated from different IPs.

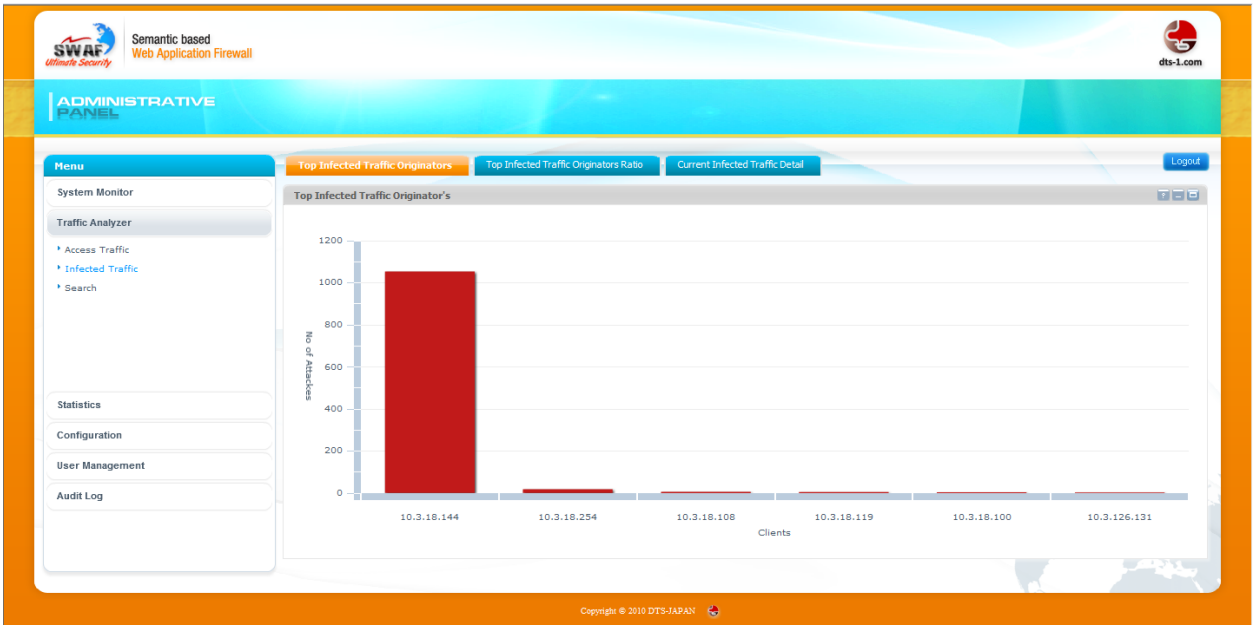

Figure 10: Top Infected Traffic Originators

2.1.3.2.2 Top Infected Traffic Originators Ratio Screen

This figure shows the ratio of Top Infected Traffic Originators.

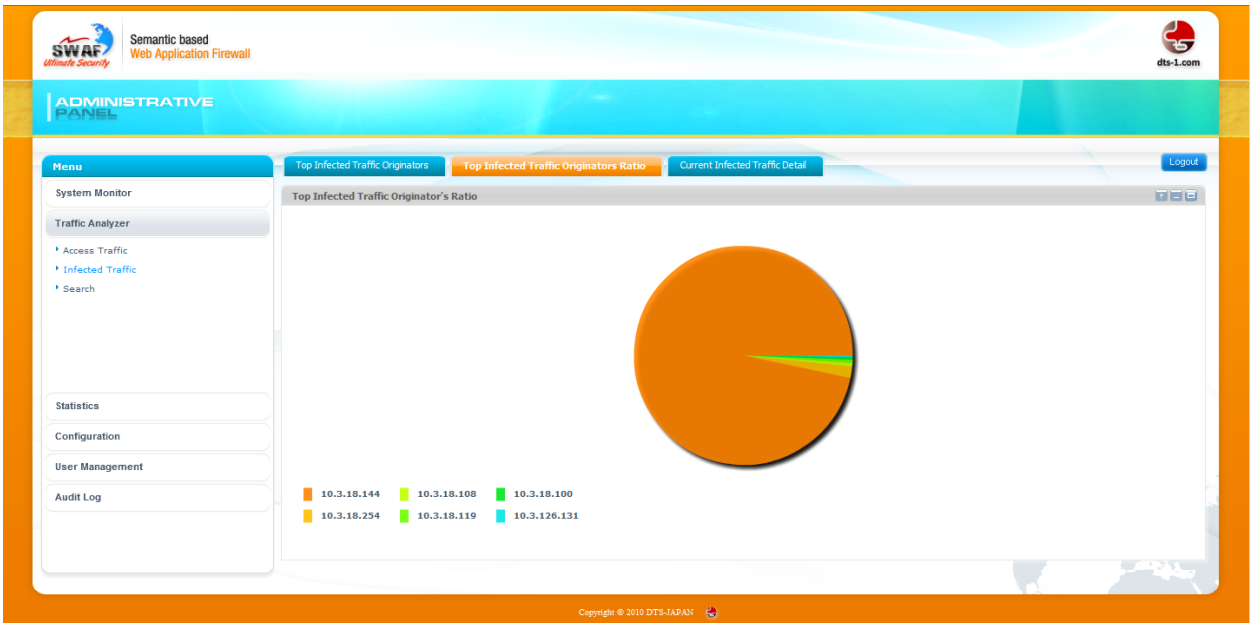

Figure 11: Top Infected Traffic Originators Ratio

2.1.3.2.3 Current Infected Traffic Detail Screen

This screen shows the whole detail of current infected Traffic.

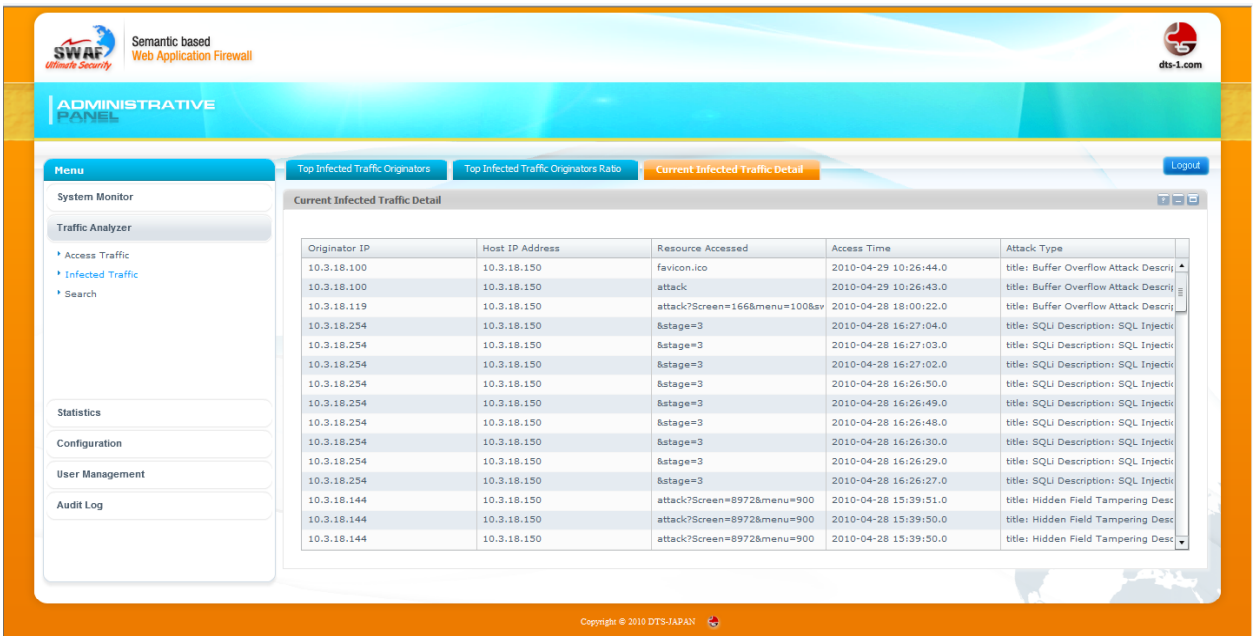
Semantic based
Web Application Firewall
dts-1.com
ADMINISTRATIVE
PANEL
Menu
System Monitor
Traffic Analyzer
Access Traffic
Infected Traffic
Search
Statistics
Configuration
User Management
Audit Log
Top Infected Traffic Originators
Top Infected Traffic Originators Ratio
Current Infected Traffic Detail
Logout
Current Infected Traffic Detail
Originator IP | Host IP Address | Resource Accessed | Access Time | Attack Type
10.3.18.100 | 10.3.18.150 | favicon.ico | 2010-04-29 10:26:44.0 | title: Buffer Overflow Attack Descri
10.3.18.100 | 10.3.18.150 | attack | 2010-04-29 10:26:43.0 | title: Buffer Overflow Attack Descri
10.3.18.119 | 10.3.18.150 | attack?Screen=166&menu=100&sv | 2010-04-28 18:00:22.0 | title: Buffer Overflow Attack Descri
10.3.18.254 | 10.3.18.150 | &stage=3 | 2010-04-28 16:27:04.0 | title: SQLi Description: SQL Injecti
10.3.18.254 | 10.3.18.150 | &stage=3 | 2010-04-28 16:27:03.0 | title: SQLi Description: SQL Injecti
10.3.18.254 | 10.3.18.150 | &stage=3 | 2010-04-28 16:27:02.0 | title: SQLi Description: SQL Injecti
10.3.18.254 | 10.3.18.150 | &stage=3 | 2010-04-28 16:26:50.0 | title: SQLi Description: SQL Injecti
10.3.18.254 | 10.3.18.150 | &stage=3 | 2010-04-28 16:26:49.0 | title: SQLi Description: SQL Injecti
10.3.18.254 | 10.3.18.150 | &stage=3 | 2010-04-28 16:26:48.0 | title: SQLi Description: SQL Injecti
10.3.18.254 | 10.3.18.150 | &stage=3 | 2010-04-28 16:26:30.0 | title: SQLi Description: SQL Injecti
10.3.18.254 | 10.3.18.150 | &stage=3 | 2010-04-28 16:26:29.0 | title: SQLi Description: SQL Injecti
10.3.18.254 | 10.3.18.150 | &stage=3 | 2010-04-28 16:26:27.0 | title: SQLi Description: SQL Injecti
10.3.18.144 | 10.3.18.150 | attack?Screen=8972&menu=900 | 2010-04-28 15:39:51.0 | title: Hidden Field Tampering Desc
10.3.18.144 | 10.3.18.150 | attack?Screen=8972&menu=900 | 2010-04-28 15:39:50.0 | title: Hidden Field Tampering Desc
10.3.18.144 | 10.3.18.150 | attack?Screen=8972&menu=900 | 2010-04-28 15:39:50.0 | title: Hidden Field Tampering Desc
Copyright © 2010 DTS-JAPAN

Figure 12: Current Infected Traffic Detail

2.1.3.3 Search Menu:

This menu gives the option to search for desired information related to access and infected log.

2.1.3.3.1 Access Log Search

This screen shows the access log which provides search on the following:

Protocol: HTTP

Method: Get/Post

Originator IP: the IP address of client

Host IP address: which is Application Server

Resource Accessed: Tells how many hits

Access Time: time allotted for resource accessed

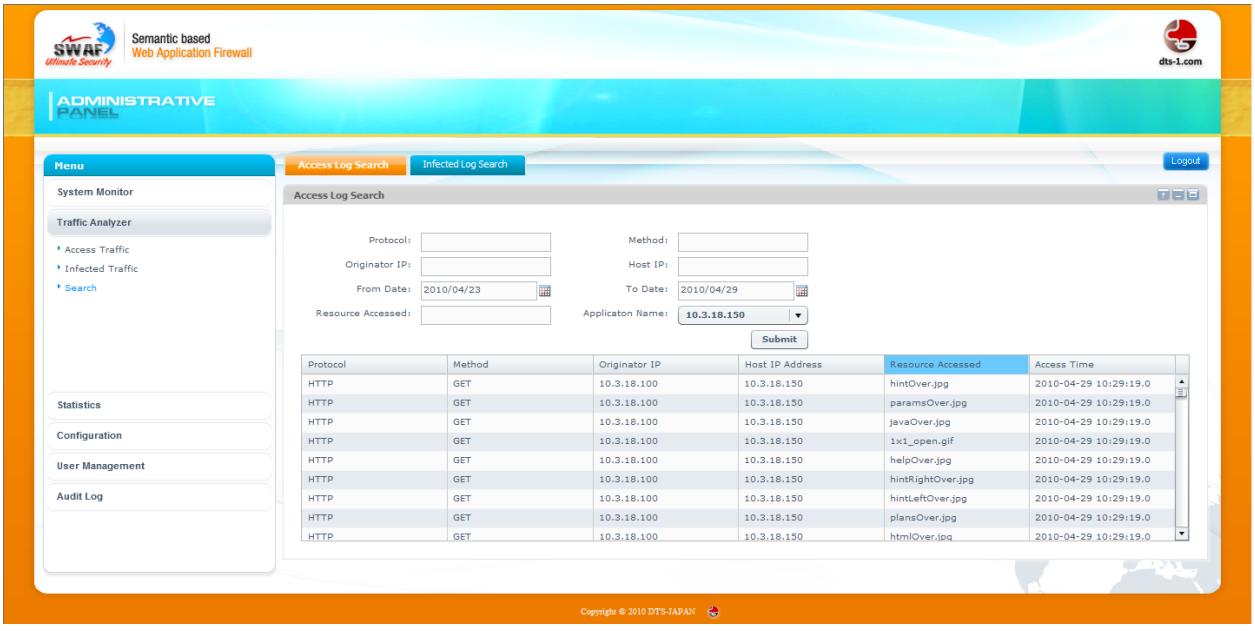

Figure 13: Access Log Search

2.1.3.3.2 Infected Log Search Screen:

This screen shows infected log search which provides search on the following:

Protocol: HTTP

Method: Get/Post

Originator IP: the IP address of client

Host IP address: which is Application Server

Resource Accessed: Tells how many hits

Attack Type: shows the type of attack i.e. XSS, DOS

From Date: shows the infected log from this date

To Date: shows the infected log till this date

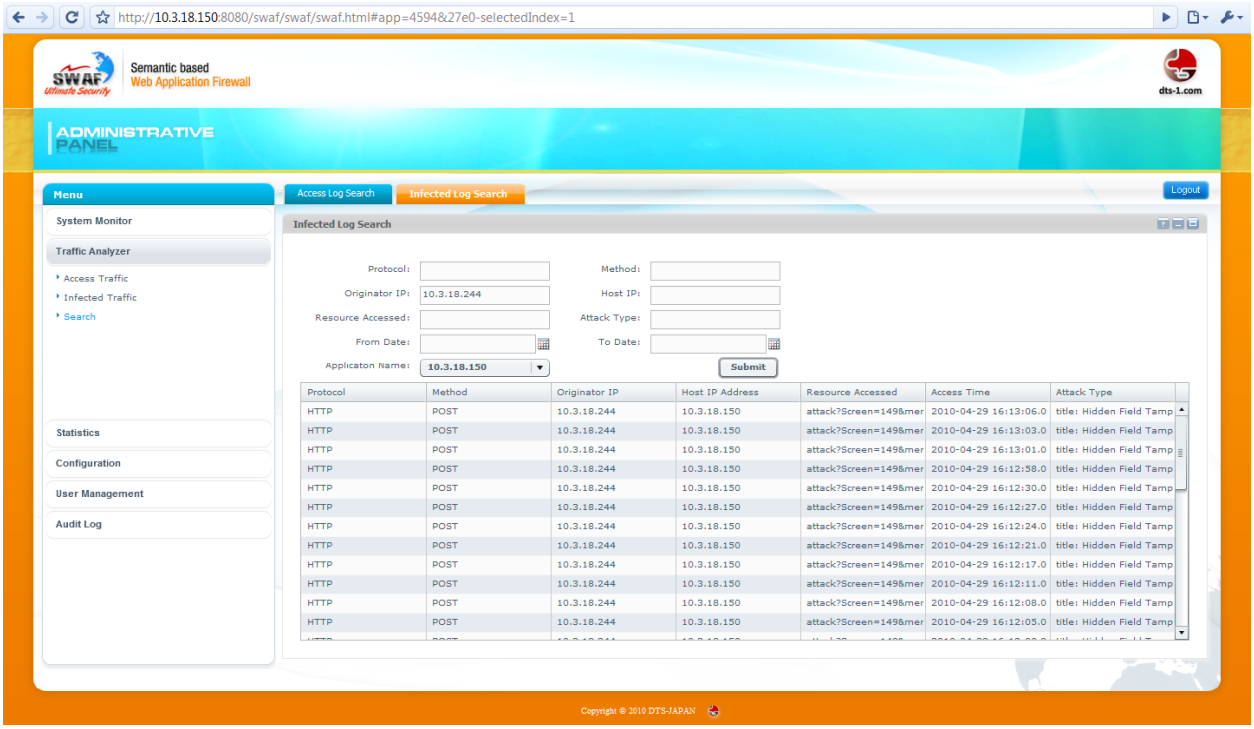

Figure 14: Current Infected Traffic Details

2.1.4 Statistics Menu:

The statistics Menu facilitates the administrator to analyze the statistical information related to access and infected traffic.

2.1.4.1 Access Traffic Menu

The access traffic menu enables the administrator to view statistics related to access traffic.

2.1.4.1.1 Access Traffic:

The screenshot below shows the bar chart for the access traffic generated by the clients. The administrator can select the dates for which he wants to view the statistics for. The screen also provides the facility of specifying the duration for which the statistics need to be displayed in the chart. After specifying the required information the administrator submits the request to the system which then displays the chart on the basis of the given information. The printing option is also available on the screen. The

administrator can press the Print button to take a print the chart displayed on the screen.

Figure 15: Access Traffic

2.1.4.1.2 Access Traffic Ratio:

This Figure shows another representation of above figure. This screen shows the pie chart to identify the ratio of access traffic generated by different clients.

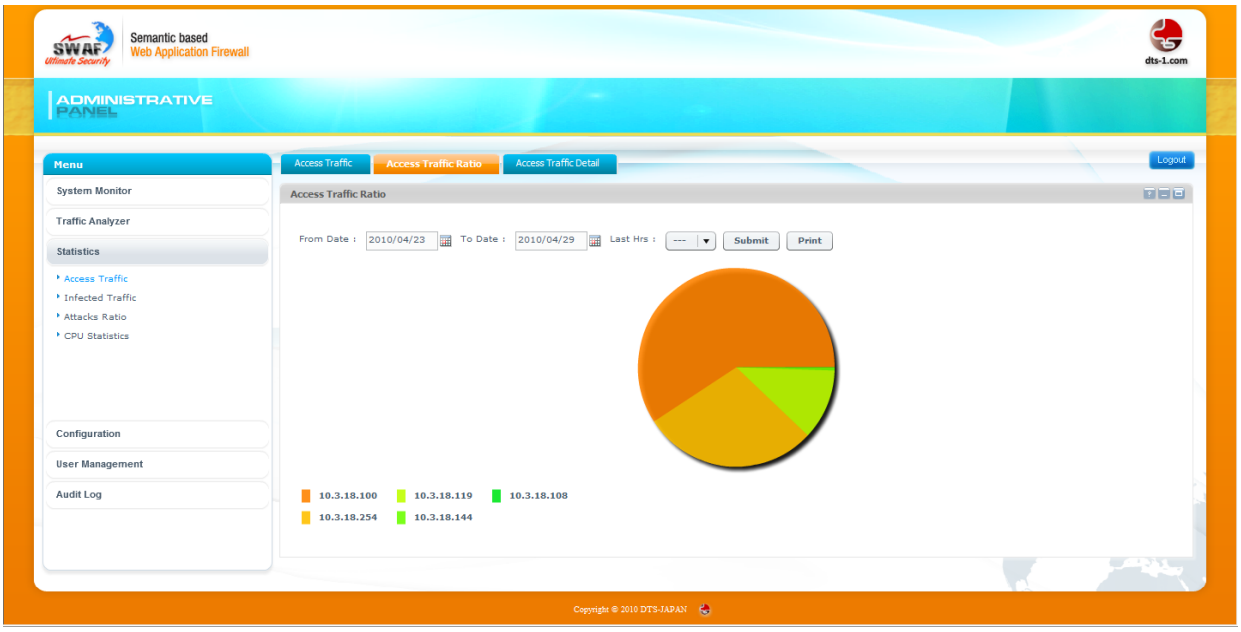

Figure 16: Access Traffic Ratio

2.1.4.1.3 Access Traffic Detail:

This figure shows the details of normal traffic which is being accessed by different IPs.

Originator IP Address: The IP address of the client machine.

Originator's Country Name: The country name of the client.

Host IP Address: The Application Server for which the requests are generated.

Resource Accessed: The resource for which the request is generated.

Access Time: The time at which the request arrived.

'Reserved' in Country name means that a public IP address is accessing the system.

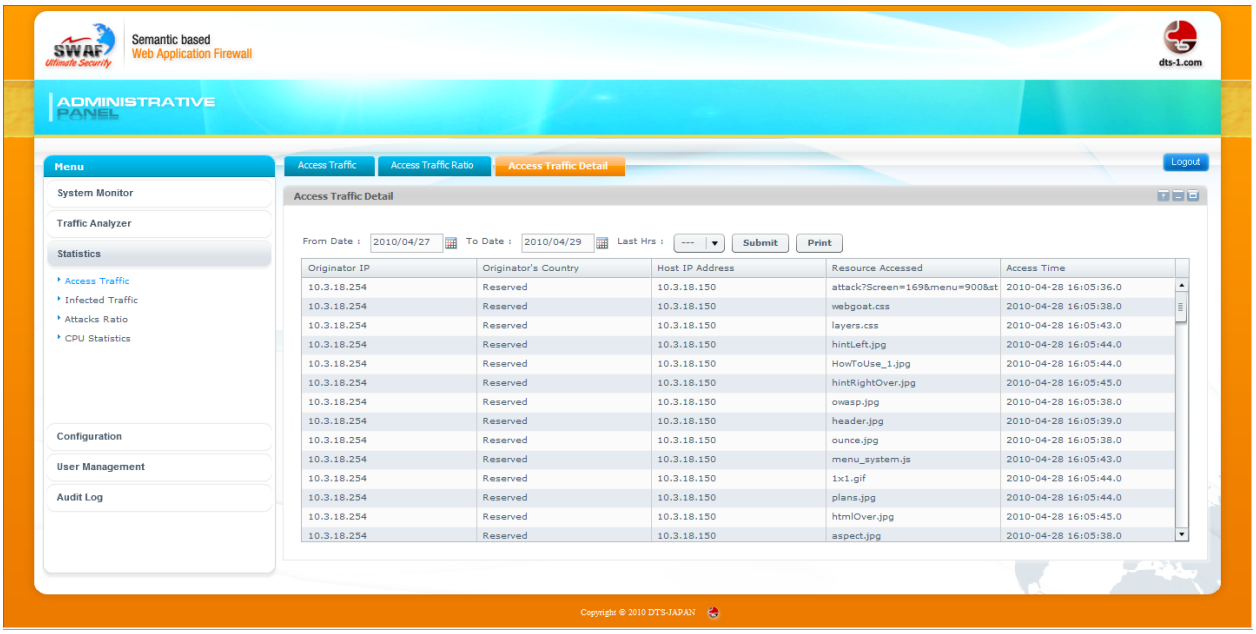

Figure 17: Access Traffic Details

2.1.4.2 Infected Traffic Menu

Infected traffic menu facilitates the administrator to view statistics related to infected log.

2.1.4.2.1 Infected traffic:

Figure shows the infected traffic generated by different IP addresses during the start and end date specified by the user.

Figure 18: Infected Traffic

2.1.4.2.2 Infected Traffic Ratio Screen:

It is another representation of above Figure

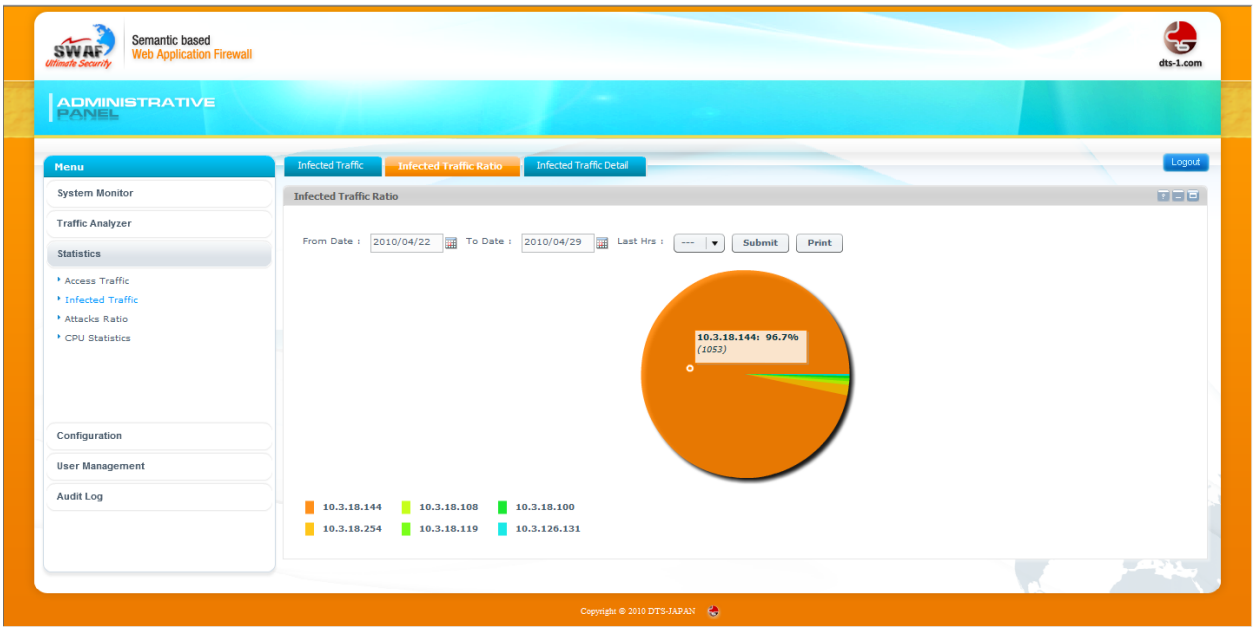

Figure 19: Infected Traffic Ratio

2.1.4.2.3 Infected Traffic Details Screen:

Figure 22 shows the details of normal traffic.

Originator IP Address: The IP address of the client machine.

Originator's Country Name: The country name of the client.

Host IP Address: The Application Server for which the requests are generated.

Resource Accessed: The resource for which the request is generated.

Access Time: The time at which the request arrived.

'Reserved' in Country name means that a public IP address is accessing the system.

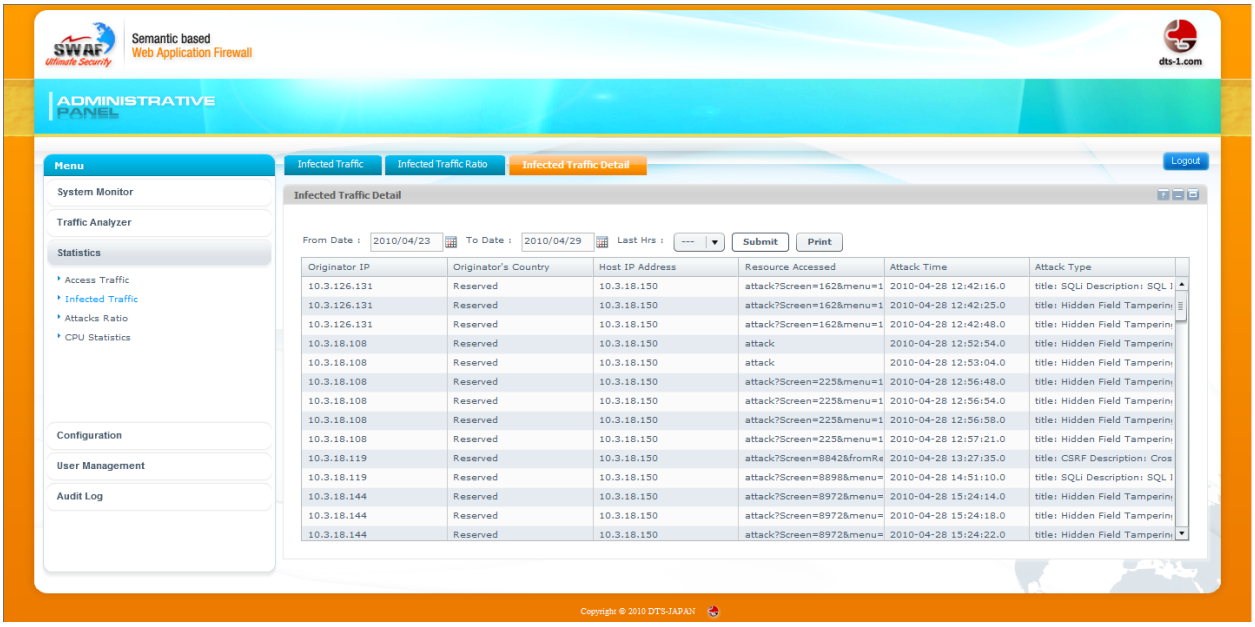
Semantic based
Web Application Firewall
dts-1.com
ADMINISTRATIVE PANEL
Menu
System Monitor
Traffic Analyzer
Statistics
Access Traffic
Infected Traffic
Attacks Ratio
CPU Statistics
Configuration
User Management
Audit Log
Infected Traffic
Infected Traffic Ratio
Infected Traffic Detail
Logout
Infected Traffic Detail
From Date : 2010/04/23
To Date : 2010/04/29
Last Hrs :
Submit
Print
Originator IP
Originator's Country
Host IP Address
Resource Accessed
Attack Time
Attack Type
10.3.126.131 Reserved 10.3.18.150 attack?Screen=162&menu=1 2010-04-28 12:42:16.0 title: SQLi Description: SQL
10.3.126.131 Reserved 10.3.18.150 attack?Screen=162&menu=1 2010-04-28 12:42:25.0 title: Hidden Field Tamperin
10.3.126.131 Reserved 10.3.18.150 attack?Screen=162&menu=1 2010-04-28 12:42:48.0 title: Hidden Field Tamperin
10.3.18.108 Reserved 10.3.18.150 attack 2010-04-28 12:52:54.0 title: Hidden Field Tamperin
10.3.18.108 Reserved 10.3.18.150 attack 2010-04-28 12:53:04.0 title: Hidden Field Tamperin
10.3.18.108 Reserved 10.3.18.150 attack?Screen=225&menu=1 2010-04-28 12:56:48.0 title: Hidden Field Tamperin
10.3.18.108 Reserved 10.3.18.150 attack?Screen=225&menu=1 2010-04-28 12:56:54.0 title: Hidden Field Tamperin
10.3.18.108 Reserved 10.3.18.150 attack?Screen=225&menu=1 2010-04-28 12:56:58.0 title: Hidden Field Tamperin
10.3.18.108 Reserved 10.3.18.150 attack?Screen=225&menu=1 2010-04-28 12:57:21.0 title: Hidden Field Tamperin
10.3.18.119 Reserved 10.3.18.150 attack?Screen=8842&fromRe 2010-04-28 13:27:35.0 title: CSRF Description: Cros
10.3.18.119 Reserved 10.3.18.150 attack?Screen=8898&menu= 2010-04-28 14:51:10.0 title: SQLi Description: SQL
10.3.18.144 Reserved 10.3.18.150 attack?Screen=8972&menu= 2010-04-28 15:24:14.0 title: Hidden Field Tamperin
10.3.18.144 Reserved 10.3.18.150 attack?Screen=8972&menu= 2010-04-28 15:24:18.0 title: Hidden Field Tamperin
10.3.18.144 Reserved 10.3.18.150 attack?Screen=8972&menu= 2010-04-28 15:24:22.0 title: Hidden Field Tamperin
Copyright © 2010 DTS-JAPAN

Figure 20: Infected Traffic Detail

2.1.4.3 *Attacks Ratio Screen:*

Figure 23 shows different attacks generated during the start and end date given by the user and the ratio of these attacks.

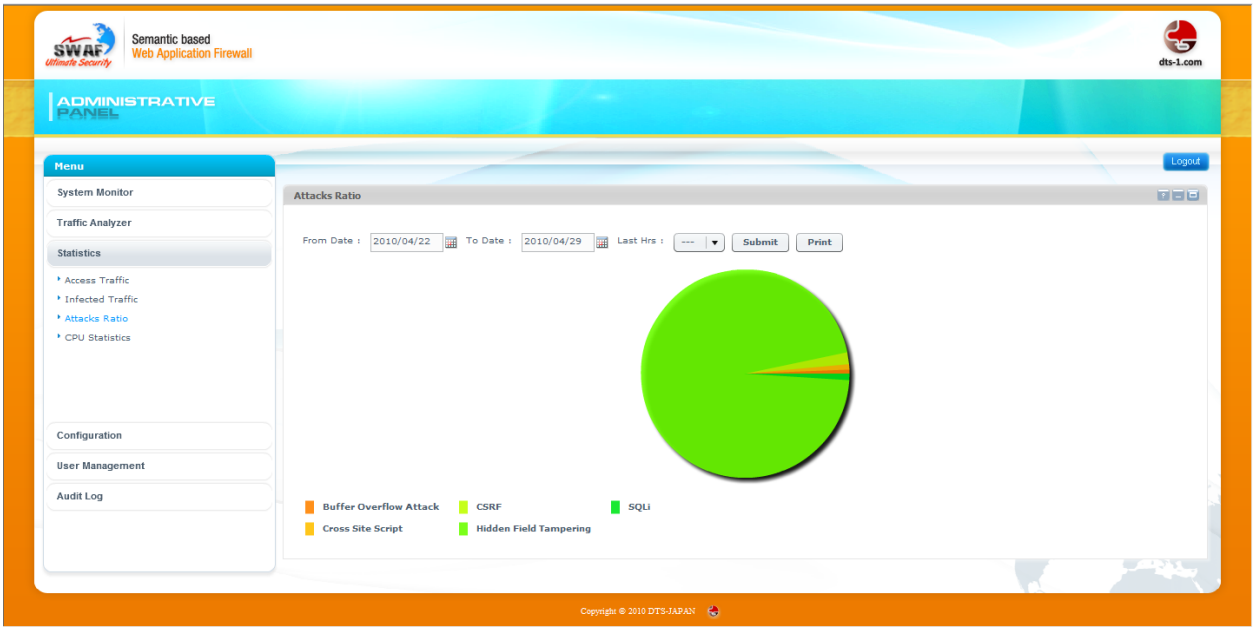

Figure 21: Attacks Ratio

2.1.4.4 CPU Statistics Screen

Figure 24 shows the statistics of CPU between two dates.

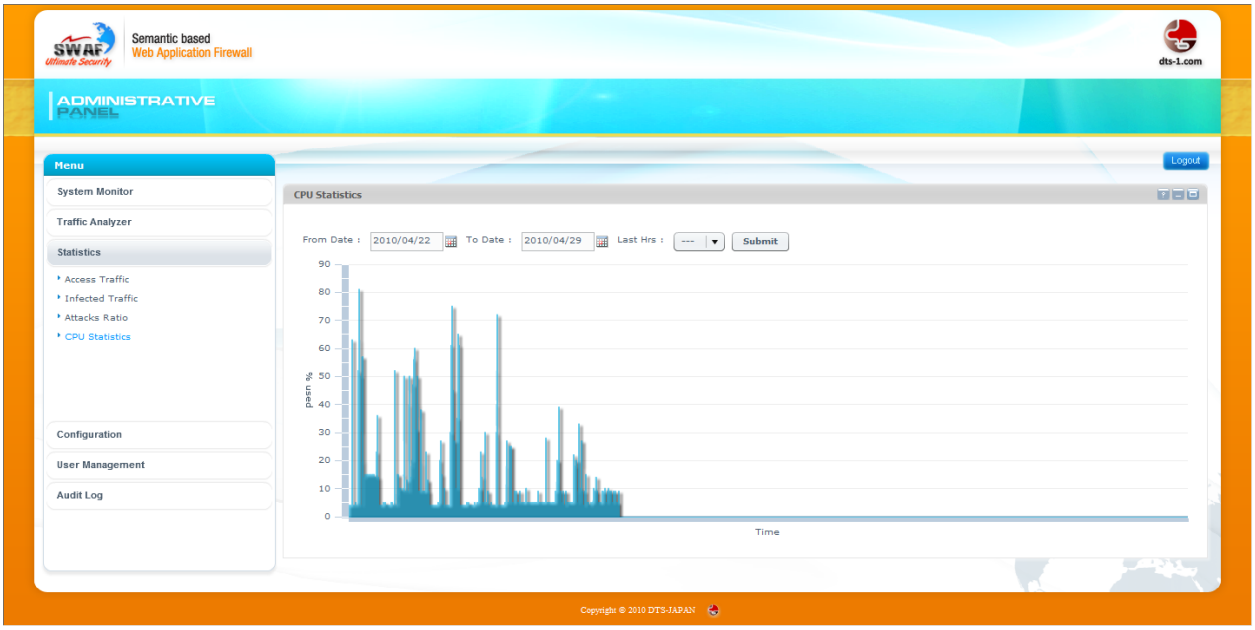

Figure 22: CPU Utilization

2.1.5 Configurations

Figure 25 shows the configuration menu can be used by administrator to set the configuration of SWAF. This menu can be used to set firewall, attack, web application, backup and rules configuration.

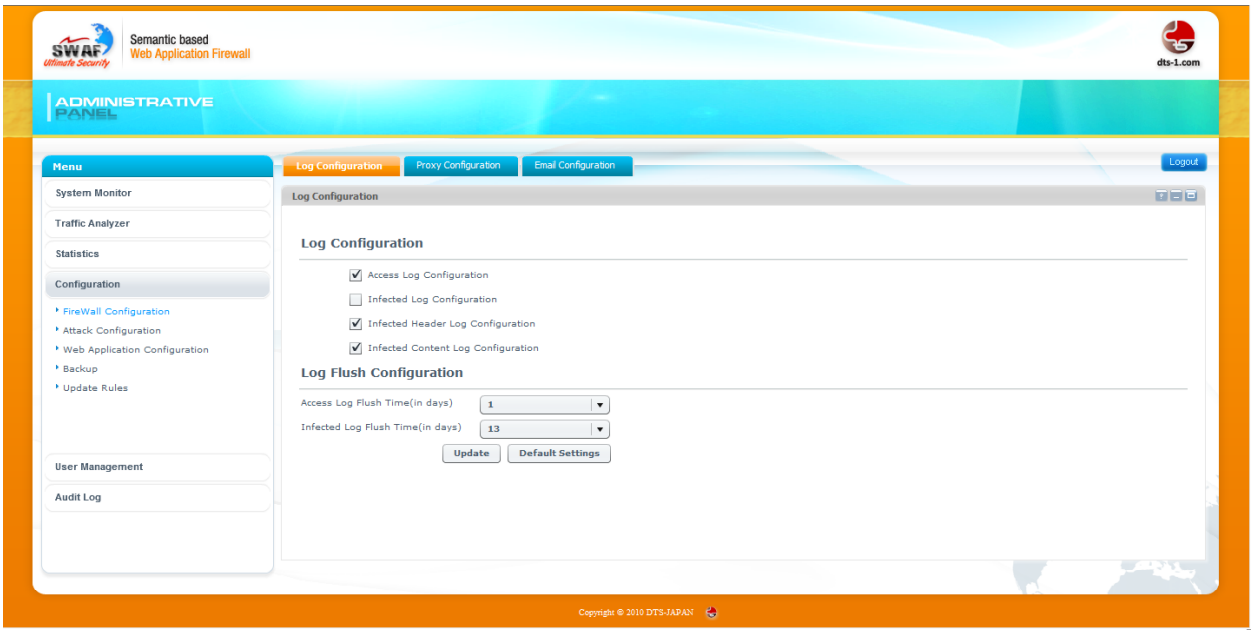

Figure 23: Configuration

2.1.5.1 Firewall Configuration Menu

Log configuration, Proxy Configuration and email configuration menus come under the firewall configuration menu. Following is the description of each sub menu:

2.1.5.1.1 Log Configuration Screen:

Figure 26 shows different log configurations tab. The first four choices show that these details of how SWAF will be store log.

Log Configuration:

Access log Configuration: It is use to log the normal traffic.

Infected log Configuration: It is use to log the malicious traffic.

Infected Header log Configuration: This option is use to log the header for the malicious requests.

Infected content log Configuration: Each HTTP request has some body. It is use to log the body of the infected traffic.

Log Flush Configuration:

Access log flush Time: After the mention days the access Traffic log will remove automatically.

Infected log flush Time: After the mention days the infected traffic log will remove automatically.

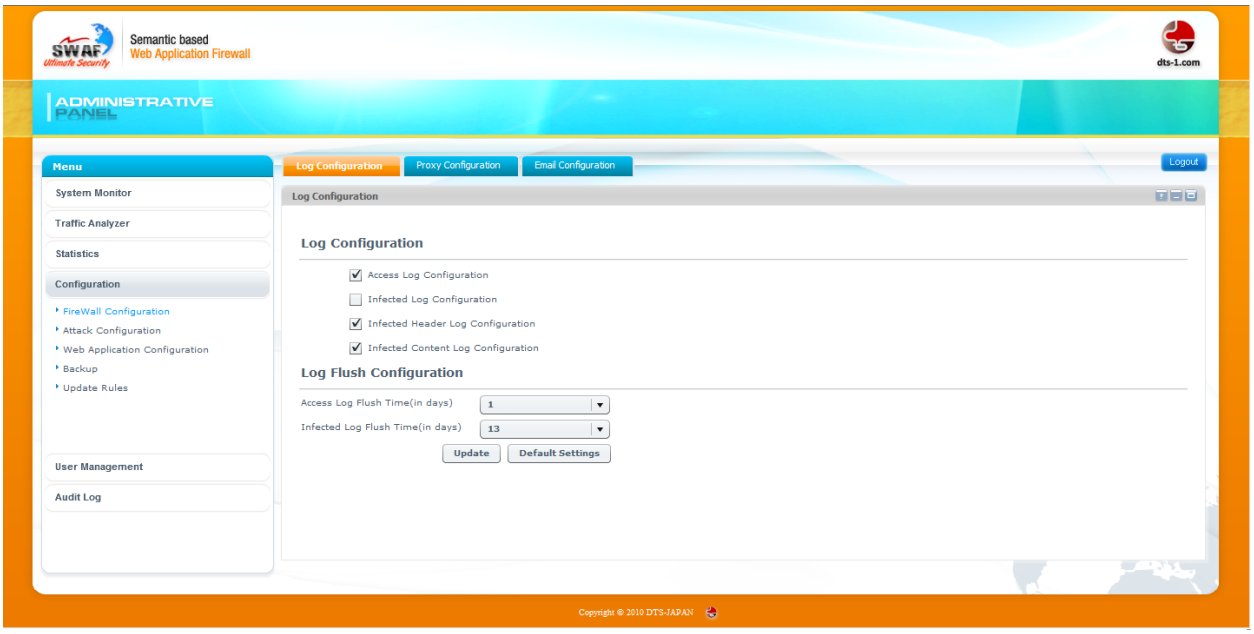

Figure 24: Log Configurations

2.1.5.1.2 Proxy Configuration Screen:

Figure 27 shows the proxy setting to the administrator. Database Configurations the administrator to set the database path, its driver, username and password.

Application Configuration

Access log pool size: It is number of threads that SWAF use to store the access traffic.

Access log batch size: It shows the capacity of each thread. When it fulls the data is transfer to the DB.

Infected log pool size: It is number of threads that SWAF use to store the infected traffic

Infected log batch size: It shows the capacity of each thread. When it fulls the data is transfer to the DB.

Access log flush (sec Time): This timer is used to automatically save data into DB from Access log Batch.

Infected log flush (sec Time): This timer is used to automatically save data into DB from Infected log Batch.

DB connection pool size: This shows the number of DB Connections that SWAF use to log the data. (Access or Infected traffic).

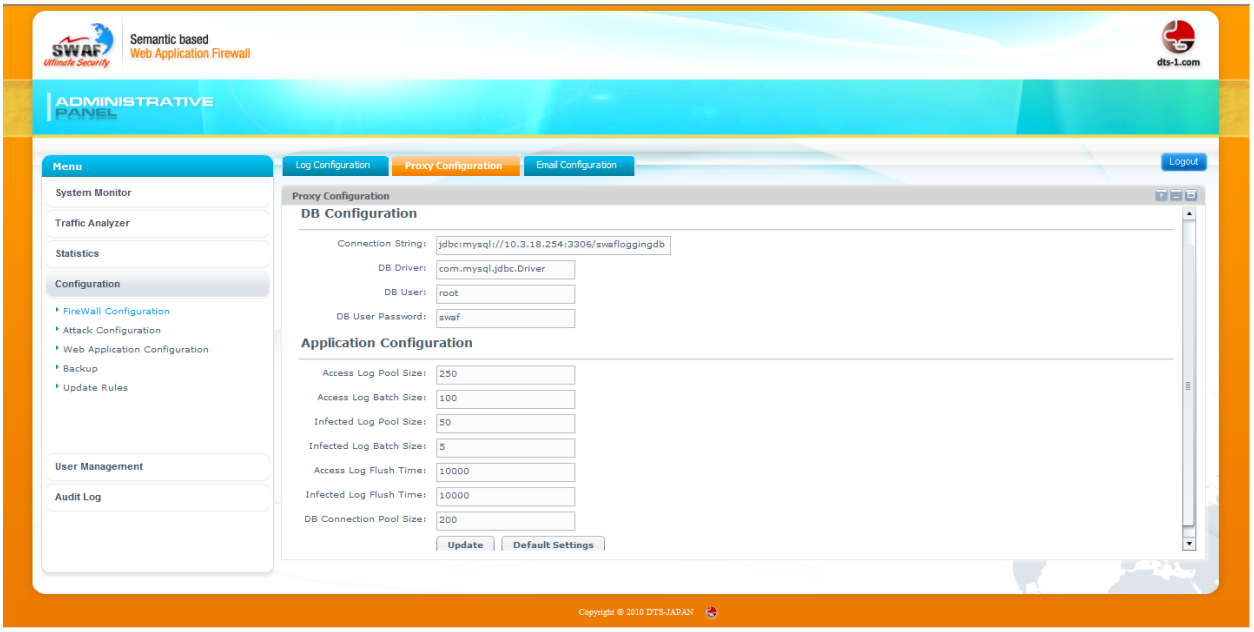

Figure 25: Proxy Configurations

2.1.5.1.3 Email Configuration Screen:

The email configuration screen provides the options to configure the e-mail server by specifying the SMTP server Address, SMTP user email and password. A check box is available to specify if the facility needs to be enabled or disabled. Following is the screenshot of the e-mail configuration screen. Following are the explanation of each option.

SMTP Server Address: It is the Address of the mailing server to receive Mails.

SMTP user email: To enter the username.

SMTP user password: To enter the password.

Confirm password: To confirm the password.

Send to: This is the address of the person or administrator who will receive the Alerts when any kind of attacks detected by SWAF.

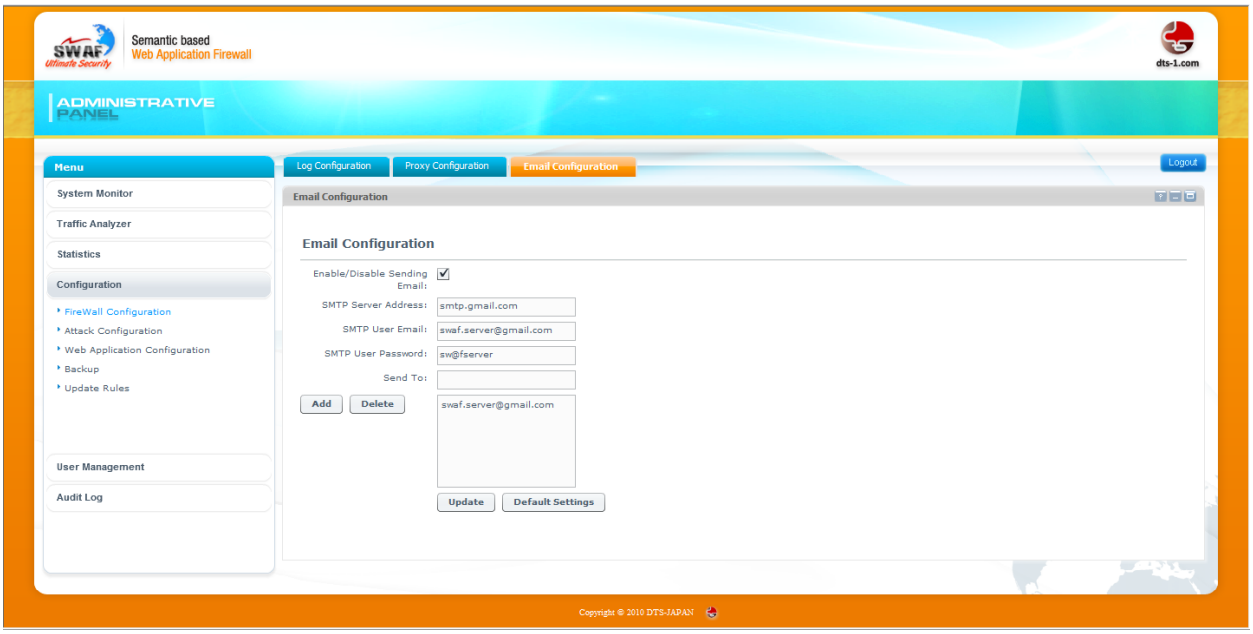

Figure 26: Email Configuration

2.1.5.2 Attack Configuration Menu:

The attack configuration menu includes screens to configure protocol validation, DOS attack and stateful attack configurations.

2.1.5.2.1 Protocol Validation Configuration Screen:

Figure 29 shows the protocol validation configurations.

Protocol Validation Configuration:

Validation Configuration:

Protocol Validation: Types of protocols that SWAF Supports e.g. HTTP, HTTPS etc.

Length Checking: Whether to check the length of header or not.

Expect header: It is a HTTP/1.1 request header using this header attacker can exploit web server vulnerabilities so administrator can uncheck to protect its web server if it has such vulnerabilities.

Request Validation: Whether the request comply the RFC 26.16 standard or not.

Response Validation: Whether the response is comply the RFC 26.16 standard or not.

Parameter Configuration:

Max Arguments: The arguments can not exceed as inputted by the administrator.

Max Headers: The headers can not exceed as inputted by the administrator.

Post parameter length: It is the length of post parameter.

Query parameter length: It is the length of query parameter.

Max header name: The header name cannot exceed the inputted value.

Max header value: The header value cannot exceed the inputted value.

Max URI length: The maximum length of URI (Universal Resource Identifier).

Max request body: The maximum HTTP body length.

HTTP Configuration:

HTTP versions: It receives only requests these three versions if all checkboxes are check otherwise if any checkbox is uncheck it will not receive the requests of that particular version.

HTTP methods: It will receive only the checked methods Requests.

Exceptions:

Disallowed file types: Disallowed those files which are add by the Administrator.

Allow redirection website: Allow the request redirection to the given website.

.

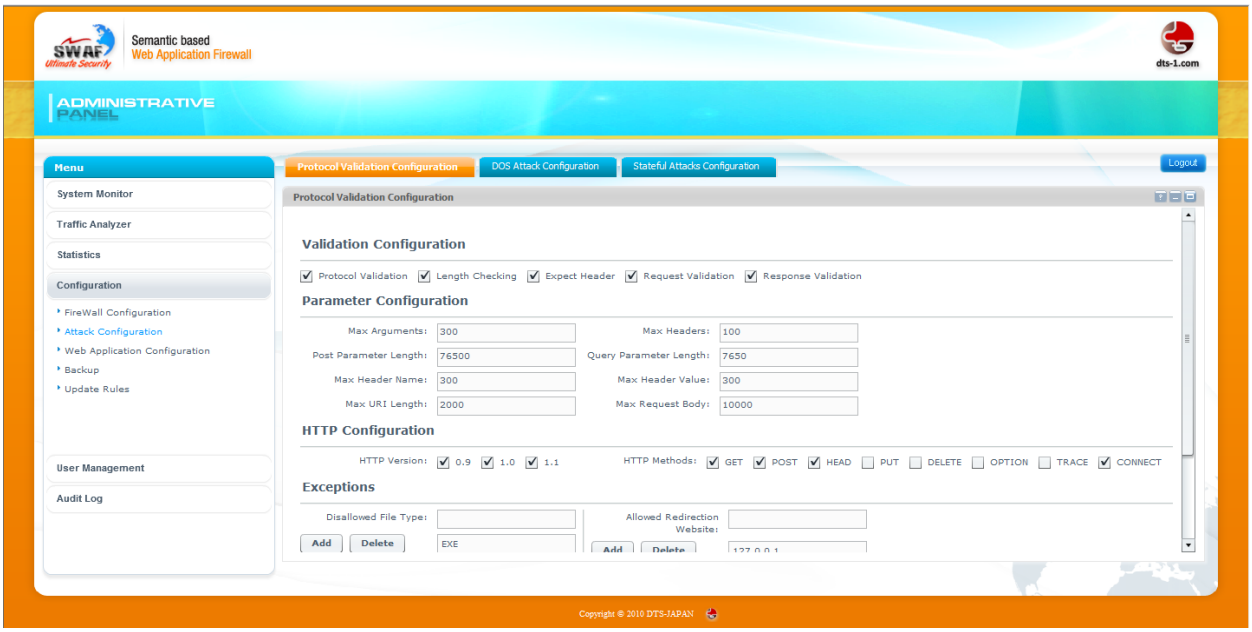

Figure 27: Protocol Validation Configurations

2.1.5.2.2 DOS Attack Configuration Screen:

Figure 30 shows the details of DOS (Denial of Service) attack.

Dos Configuration:

Enable/ Disable Dos: Enable will stop the Dos attack and disable will not stop the Dos attack

Concurrent requests/second: The overall requests send by the user to Web Server. If it exceeds the given value it will be denied.

Concurrent requests user/second: The maximum requests send by the user to a single page if it exceeds it will be denied.

Blocking time in seconds: The time in which user is block to send more requests.

Exceptions:

Allowed IP/Allowed traffic: Allow the traffic against the given IP.

Allowed resource/Allowed resource traffic: Allow the traffic against the Allowed resource.

.

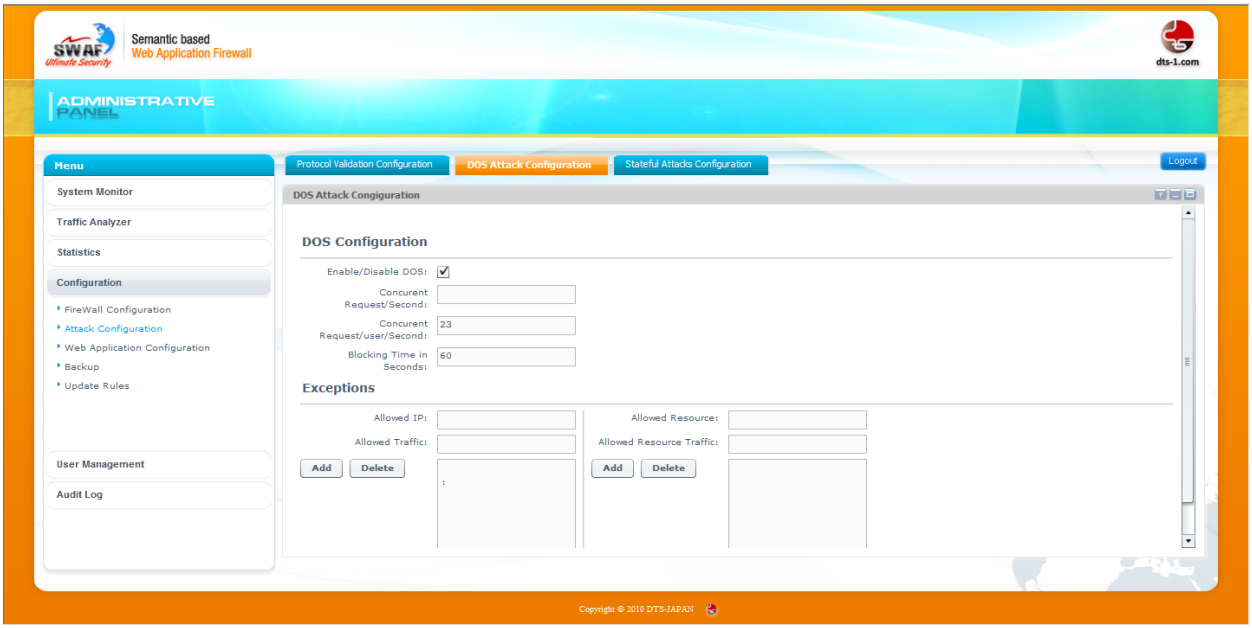

Figure 28: DoS Configurations

2.1.5.2.3 Stateful Attacks Configuration:

The stateful attack configuration screen provides configuration facility for attacks such as CSRF and hidden field exploits which require the state of the application to be maintained on SWAF. The check boxes provide the options to state if the state needs to be maintained and to specify the type of attack for which the state needs to be maintained. Additionally incase of CSRF protection, the token that needs to be provided to authenticate request and its properties can also be configured using this screen.

Manage State: It manages the user session state.

Protect CSRF: If this option is checked SWAF will protect the web server from CSRF attack.

Protect hidden: If this option is checked SWAF will protect the web server from hidden field attack.

Token Name: It is the name of the token through which client is identified.

Expiration Time (in minutes): The session maintain for how much time and after this time the session will ended automatically

Cookies life (in days): After how much days the cookies will remove.

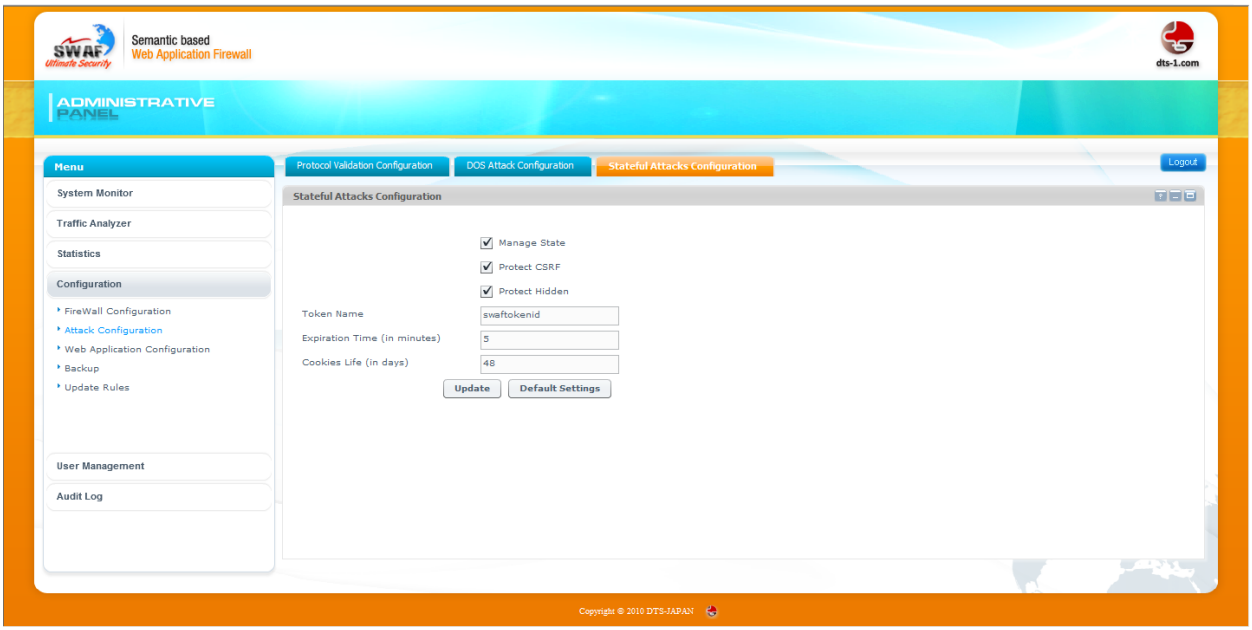

Figure 29: Stateful Attacks Configuration

2.1.5.3 Web Application Configuration Screen:

Figure 32 shows the number of application servers running behind SWAF, their IP addresses, the port on which they are listening and if the application uses HTTPS.

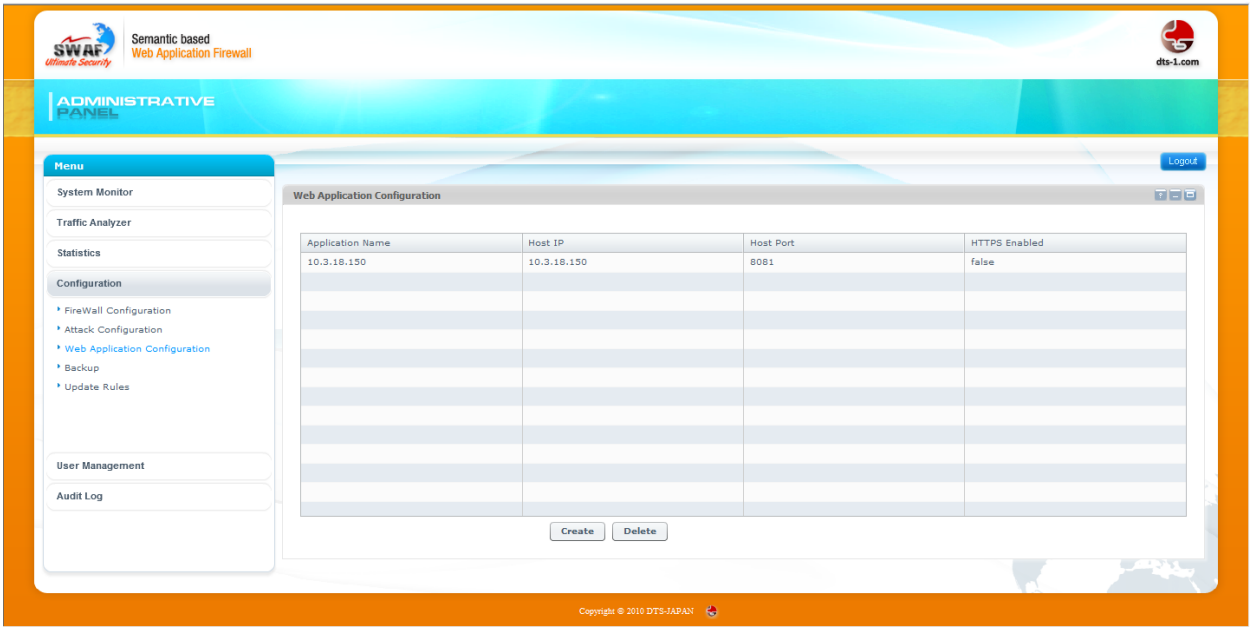

Figure 30: Web Application Configurations

2.1.5.4 Backup

The backup menu has two further tabs the configuration backup tab and the DB backup tab. The detail for each is provided below:

2.1.5.4.1 DB Backup:

The DB backup configuration screen provides the option to configure and restore Database Backup. To create a DB backup the administrator needs to press on the Backup Now button and to restore the backup the administrator needs to select the specific backup from the Backup list and press the Restore button.

Backup now: When it is clicked backup of database is created.
26 05 2010 05 16 27.

dd mm yy Hr min sec

This is the format for the database backup.

Restore: When the user want to restore the backup he will click this button.

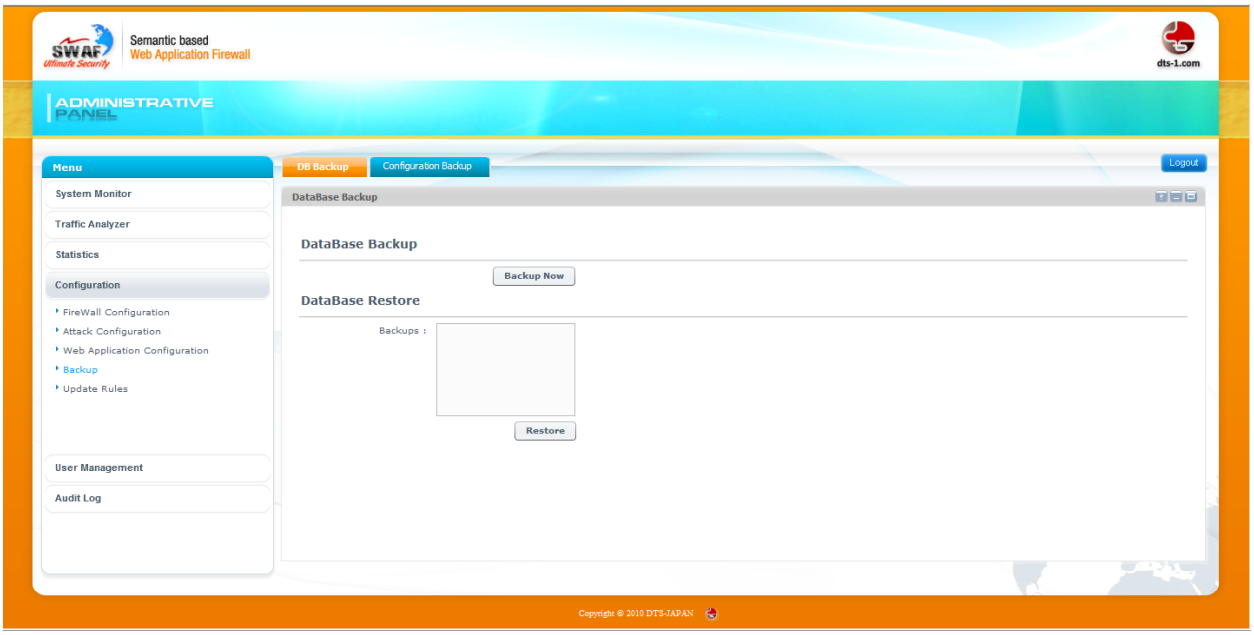

Figure 31: DB Backup

2.1.5.4.2 Configuration Backup:

The screen can be used to configure backup. The screen gives the option of providing the backup type using the dropdown list and to restore the backup at a later stage.

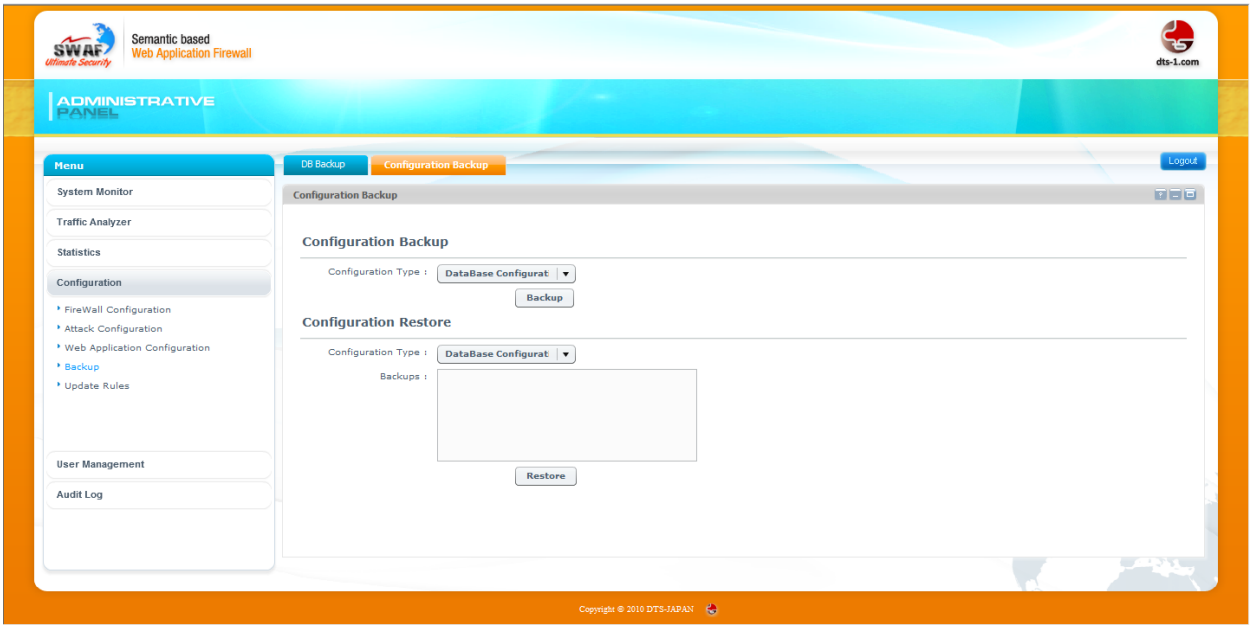

Figure 32: Configuration Backup

2.1.5.5 Update Rules:

The Update rules screen provides the option to update rule files. The administrator is required to specify his username and password to perform the update operation. The purpose of this screen is to update the knowledge base that contains the attack detection rules. The knowledgebase must be updated (if update exists the update will be provide by the swaf update server) in order to have the latest attack definition list.

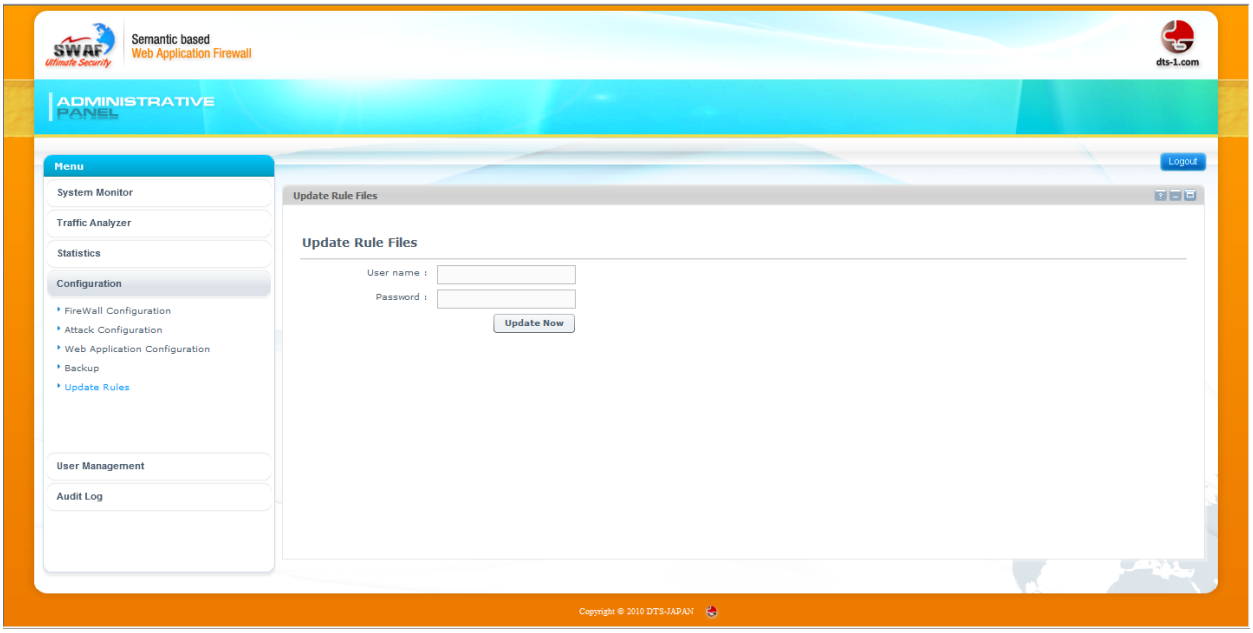

Figure 33: Update Rules Files

2.1.6 User Management

Figure 36 shows the User Management menu, which includes 2 sub menus which refer to the User Management and role rights.

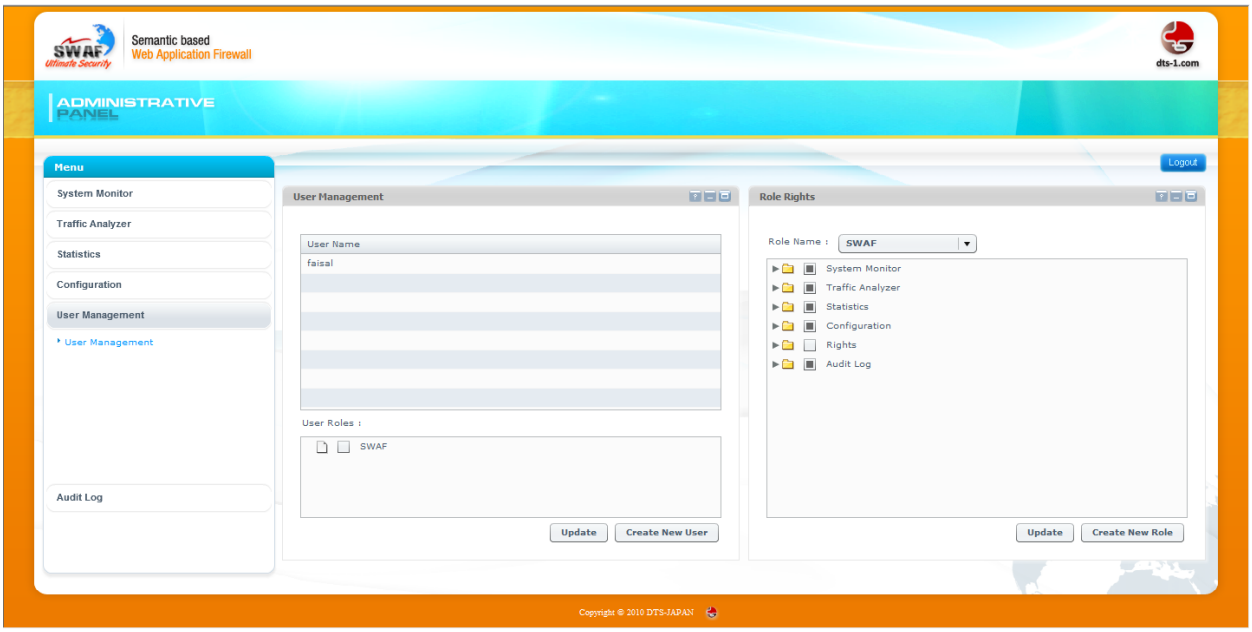

Figure 34: User Management

2.1.6.1 User Management

Figure 37 shows user management screen, update is used to change the rights of a user. New users can be created using this screen.

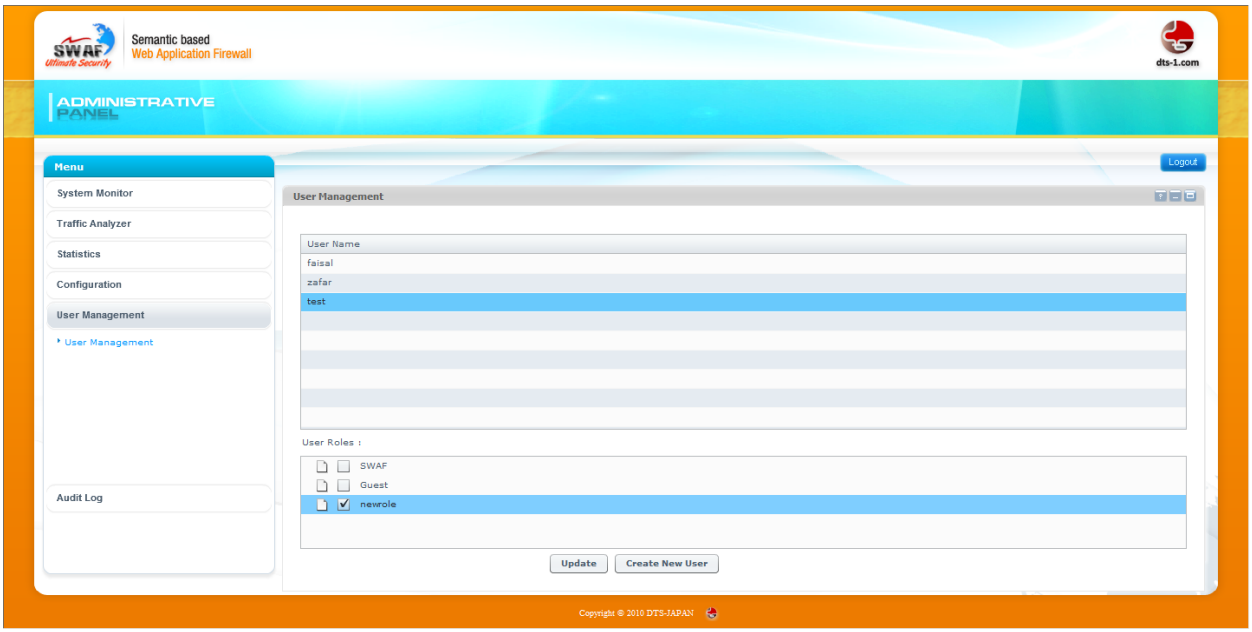

Figure 35: User Management

2.1.6.2 Role Rights Screen

Figure 38 shows the role rights which can be assigned to specific. The rights are specified and can be checked to select the rights for a given role.

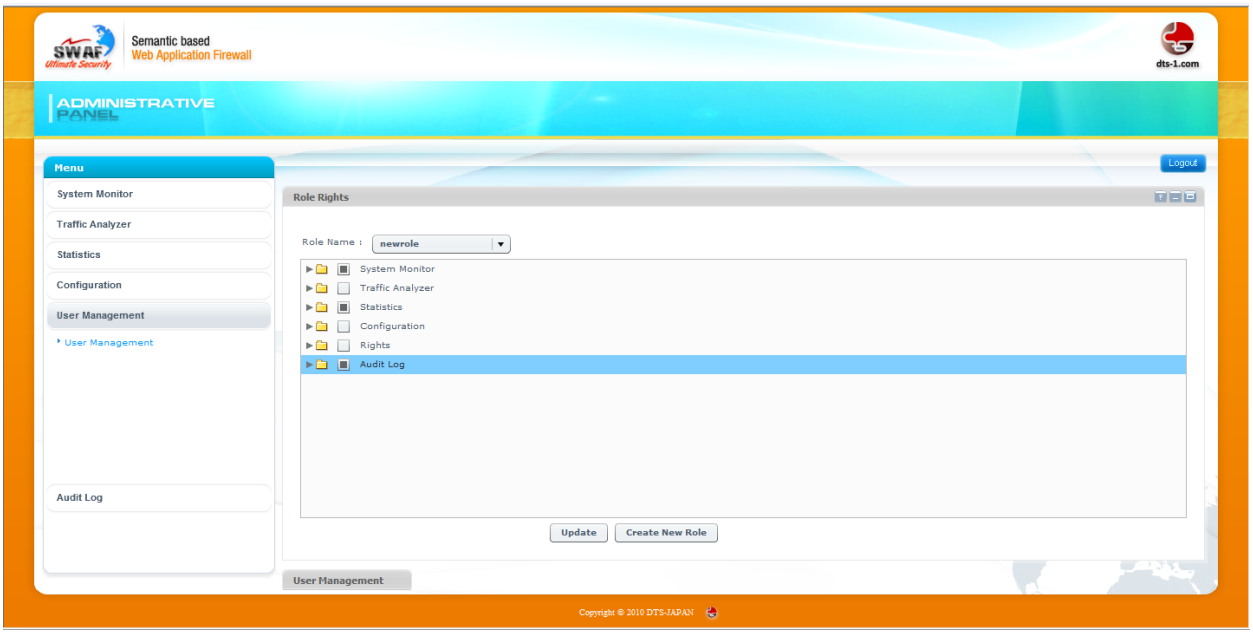

Figure 36: Group Rights

2.1.7 Audit Log Menu

Audit log menu provide information related to log present in the database. Figure 7 shows the screenshot of the audit log menu. Audit log menu comprises of two further screens the User log and the Audit log, as shown in Figure 39.

Figure 37: Audit Log

2.1.7.1 User Log Screen

Figure 40 provide the maximized view of User log screen. To view the user logs the user needs to specify the period for which he/she intends to view the log entries saved on the server. On pressing the submit button the user log for the given period can be viewed by the user.

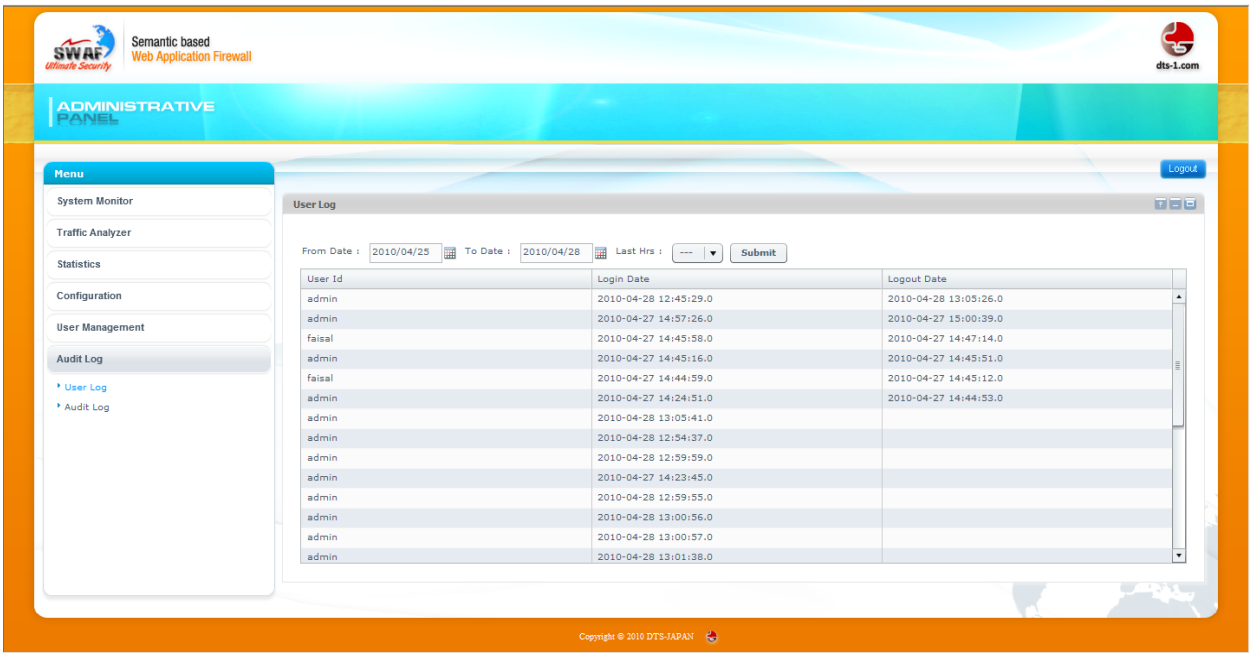

Figure 38: User Log

Figure presents the user log information provided to the user. The user log contains

User Id: Specifying the user id of user who logged into the system,

Login Date: Specifying the login date along with time and

Logout Date: Giving the logout date and time.

2.1.7.2 Audit Log Screen:

Figure 41 presents the maximized view of the audit log screen. To view the audit logs the user needs to specify the period for which he/she intends to view the audit log entries saved on the server. On pressing the submit button the audit log for the given period can be viewed by the user.

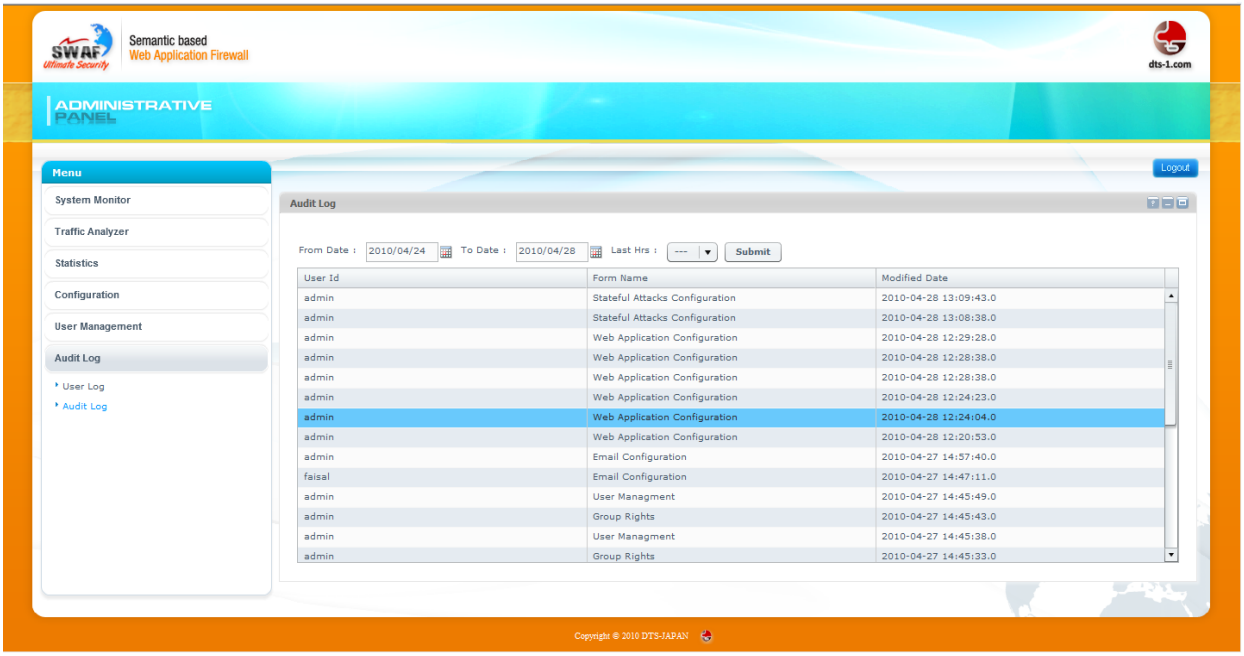
Semantic based
Web Application Firewall
dts-1.com
ADMINISTRATIVE PANEL
Menu
System Monitor
Traffic Analyzer
Statistics
Configuration
User Management
Audit Log
User Log
Audit Log
Logout
Audit Log
From Date : 2010/04/24
To Date : 2010/04/28
Last Hrs :
Submit
User Id | Form Name | Modified Date
admin | Stateful Attacks Configuration | 2010-04-28 13:09:43.0
admin | Stateful Attacks Configuration | 2010-04-28 13:08:38.0
admin | Web Application Configuration | 2010-04-28 12:29:28.0
admin | Web Application Configuration | 2010-04-28 12:28:38.0
admin | Web Application Configuration | 2010-04-28 12:28:38.0
admin | Web Application Configuration | 2010-04-28 12:24:23.0
admin | Web Application Configuration | 2010-04-28 12:24:04.0
admin | Web Application Configuration | 2010-04-28 12:20:53.0
admin | Email Configuration | 2010-04-27 14:57:40.0
faisal | Email Configuration | 2010-04-27 14:47:11.0
admin | User Managment | 2010-04-27 14:45:49.0
admin | Group Rights | 2010-04-27 14:45:43.0
admin | User Managment | 2010-04-27 14:45:38.0
admin | Group Rights | 2010-04-27 14:45:33.0
Copyright © 2010 DTS-JAPAN

Figure 39: Audit Log

Figure presents the audit log information provided to the user. The audit log screen contains the

User Id: Specifies the user id of user who logged into the system,

Form Name: Specifying the screen where changes have been done and

Modified Date: Gives the date and time on which the change has been done.

3 Case Study

This section presents the usage scenarios of SWAF; the intension is to facilitate the user in performing desired operations with ease. The first usage scenario gives a detailed

description of configuring a Web Application with SAWF. In the second Scenario the user and group creation and then the process of assigning a user to a group/ groups is described.

3.1 Example scenario # 1

This Example scenario gives a stepwise description of configuring a web application to be protected using SWAF.

3.2 Configuring a Web Application with SWAF

To configure a web application with SWAF, press the Create Button on the Web Application Configuration Screen of the Configuration Tab.

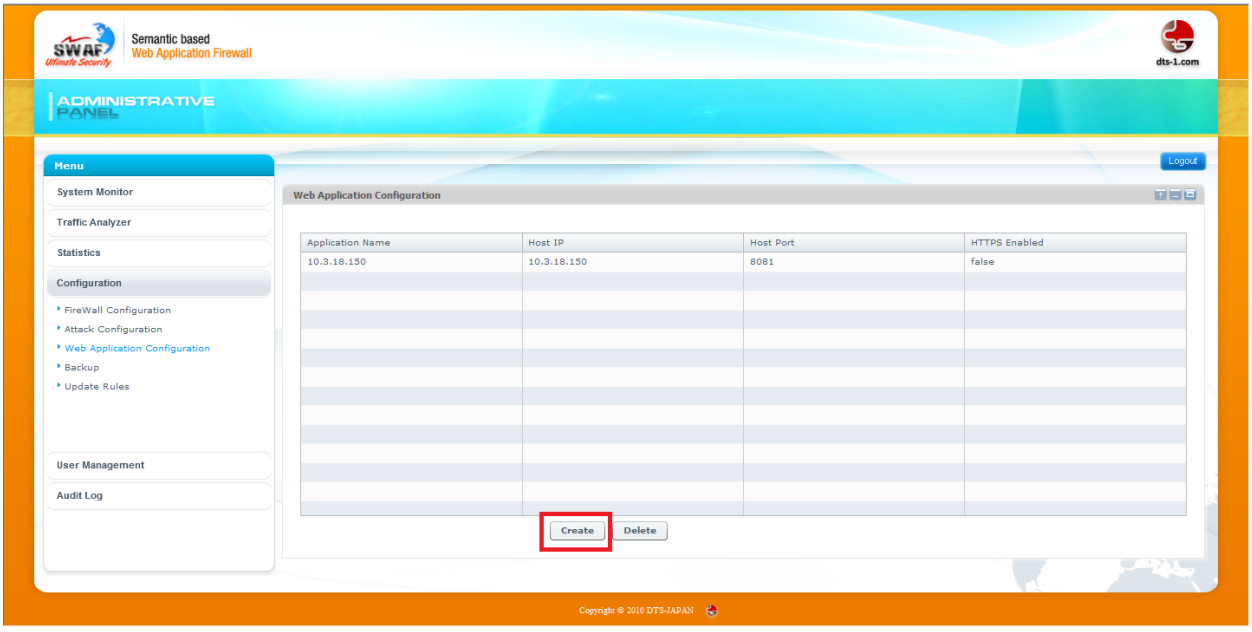

Figure 40: Web Application Configuration

A new window to specify the Web Application details appears on the screen, after specifying the required information click on the Create Button to confirm the request, following is the screenshot of the explained screen:

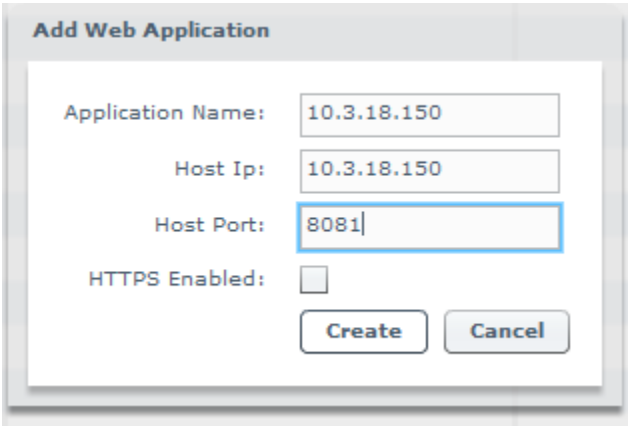

Figure 41: Add Web Application

A message box specifying the successful configuration of the Web Application is displayed on the screen.

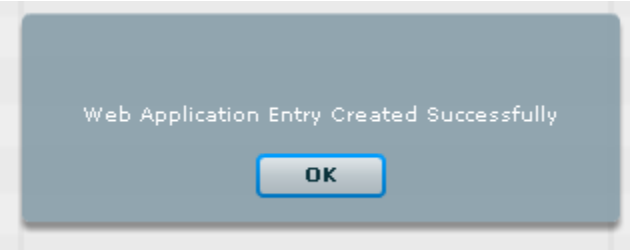

Figure 42: Successful creation of Web Application

3.3 Example scenario # 2

The following example scenario presents a stepwise description of creating a user and providing him rights by assigning him to a group or groups.

3.3.1 Creating a new user

1. To create a new user the user need to enable the User Management tab. And click on the Create New User button.

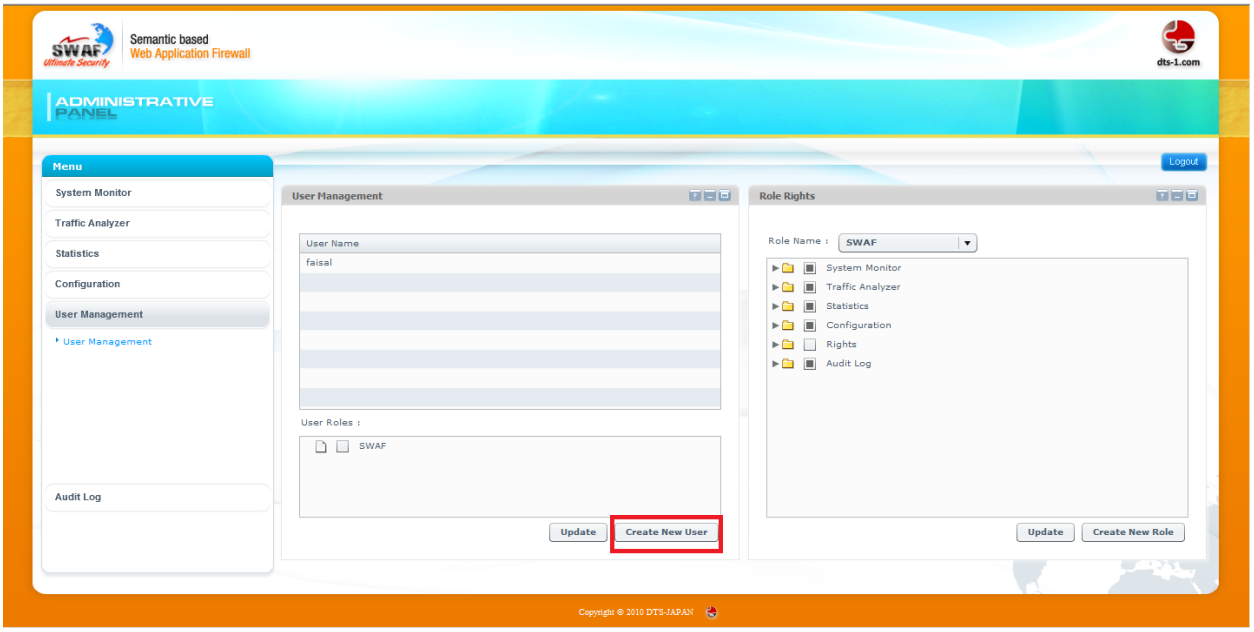

Figure 43: User Management

2. A screen to create a new user appears.

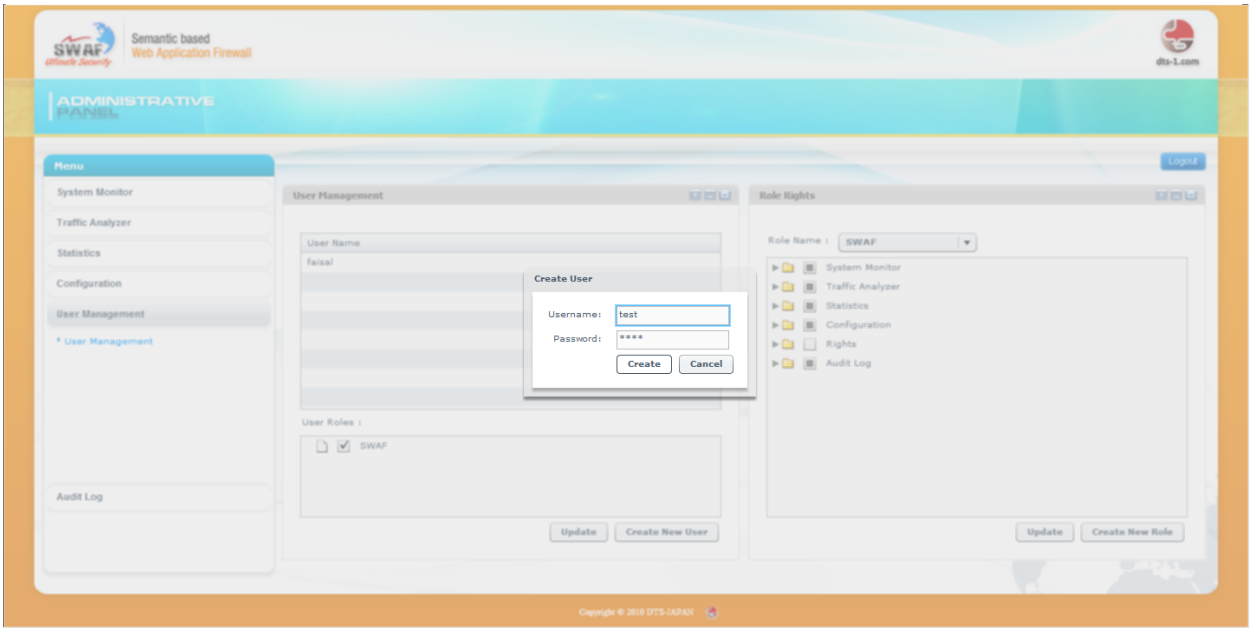

Figure 44: Create User

The administrator needs to specify the username and password for the new user and press on the create button.

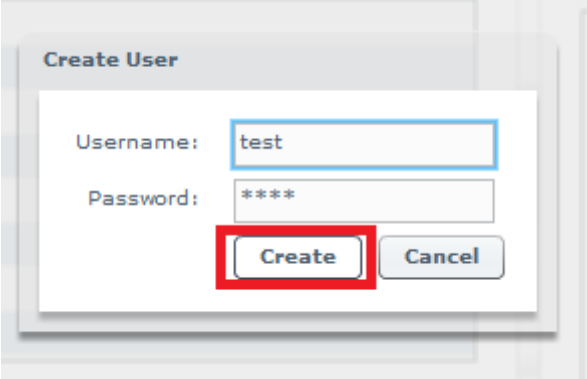

Figure 45: New User Creation

A message specifying successful creation of the user is displayed on the screen.

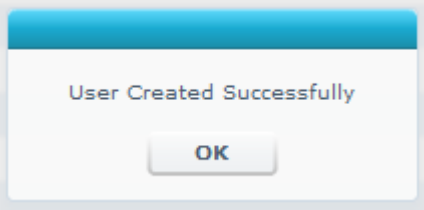

Figure 46: Successful Creation of User

3.3.2 Assigning role to a User

To assign a role to a user, select the user from the list and check mark the role from the list of User Roles given below. Press update to confirm the request.

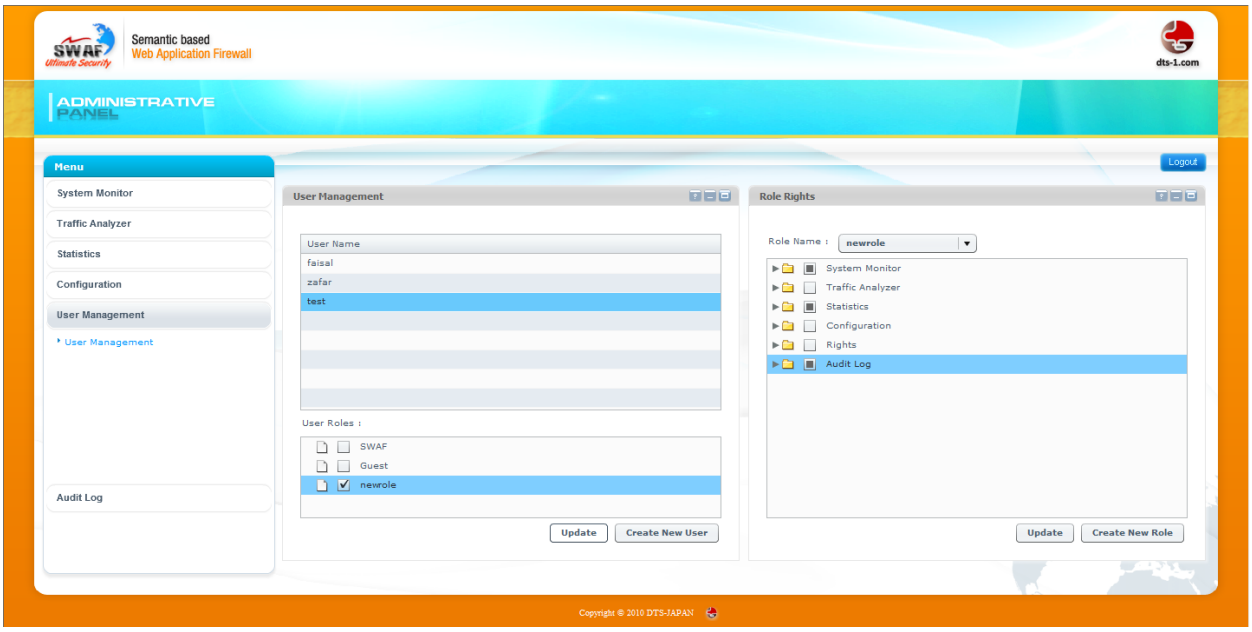

Figure 47: Role Rights

3.3.3 Creating a User Role

1. Press the Create New Role button on the Role Rights Screen.

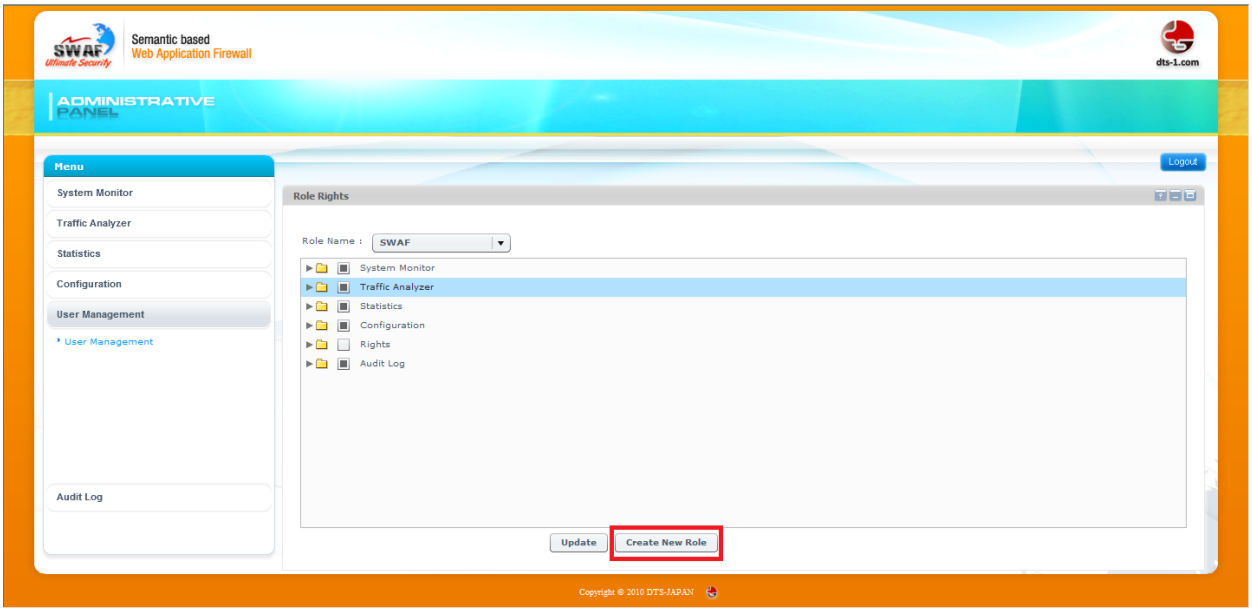

Figure 48: Creating New Role

2. A screen to specify the Role name and Role Description appears on the screen. Specify the required information and press the Create button to confirm the request.

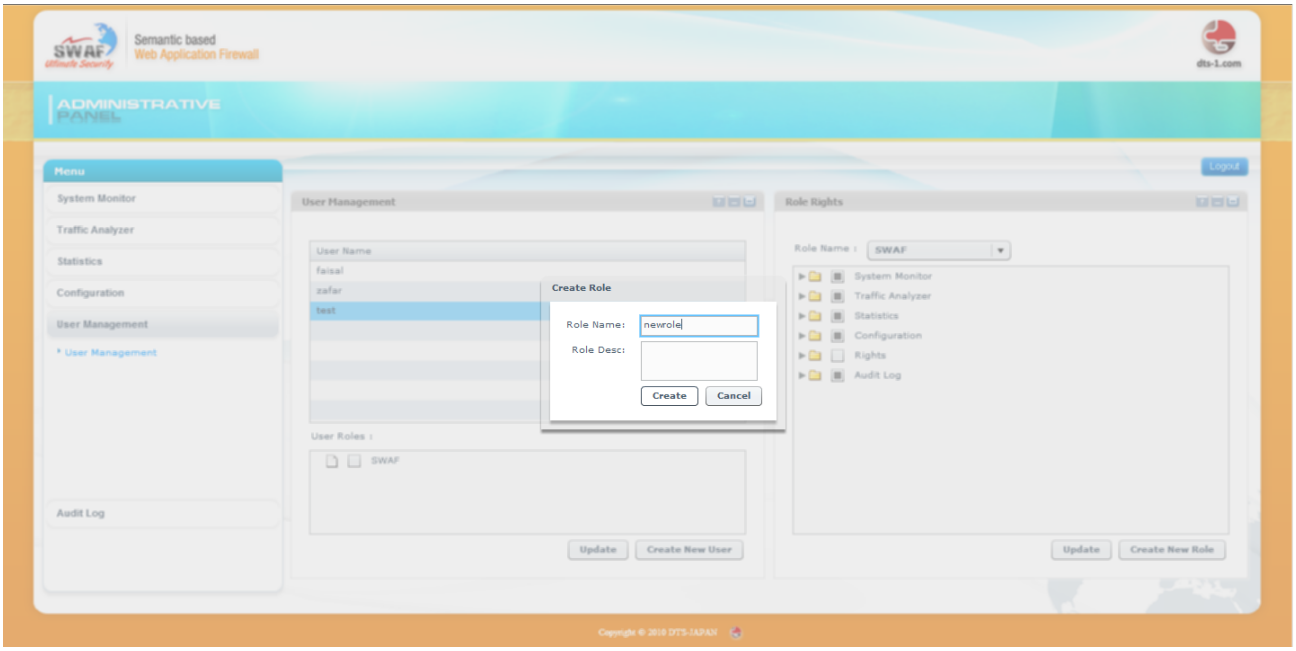

Figure 49: Create Role

A message specifying the successful creation of the group appears on the screen.

3. To assign rights to the Role, select the role from the drop down menu given on the Role Rights Screen. Check mark the rights that you want to assign to the group and press Update Button to confirm the request.

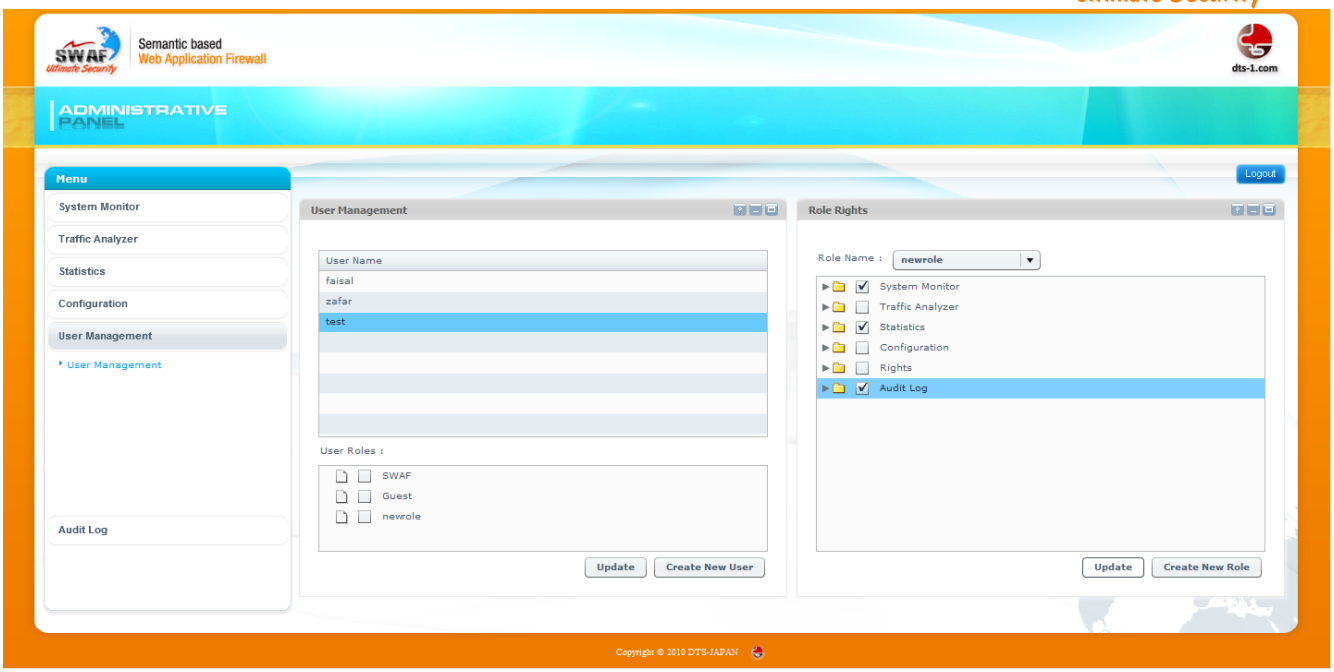

Figure 50: Assigning role to user

Glossary

Access Log: An access log is a list of all the requests for individual files that people have requested from a Web site. These files will include the HTML files and their imbedded graphic images and any other associated files that get transmitted.

Audit Log: Audit log is a chronological sequence of audit records, each of which contains evidence directly pertaining to and resulting from the execution of a business process or system function.

CPU Utilization: Whenever a hard disk is transferring data over the interface to the rest of the system, it uses some of the system's resources. One of the more critical of these resources is how much CPU time is required for the transfer. This is called the *CPU utilization* of the transfer.